Lasse Tullinen

YRITYKSEN TIETOVERKKOJEN JA KASSAJÄRJESTELMÄN PÄIVITTÄMINEN

Opinnäytetyö
Tietotekniikan koulutusohjelma

Toukokuu 2011

MIKKELIN AMMATTIKORKEAKOULU
Mikkeli University of Applied Sciences

KUVAILULEHTI

MIKKELIN AMMATTIKORKEAKOULU Mikkeli University of Applied Sciences	**Opinnäytetyön päivämäärä** 26.5.2011
Tekijä(t) Tullinen, Lasse	**Koulutusohjelma ja suuntautuminen** Tietotekniikan koulutusohjelma

Nimeke

Yrityksen tietoverkkojen ja kassajärjestelmän päivittäminen

Tiivistelmä

Opinnäytetyöni tarkoituksena oli tehdä JP-Ravintolat Oy:n toimeksiannon mukainen muutos yrityksen tietojärjestelmiin. Muutoksiin kuului yrityksen kassajärjestelmän päivittäminen sekä olemassa olevien verkkoratkaisujen yksinkertaistaminen.

Teoriaosuudessa perehdytään erilaisiin teknisiin ratkaisuihin, joilla on yritysmaailmassa mahdollista yhdistää yrityksen eri toimipaikkojen tietoverkot toisiinsa. Osuudessa tarkastellaan muun muassa sillattuja ja reititettyjä yhteyksiä sekä perehdytään VPN-verkkoihin. Lisäksi esitellään eri vaihtoehtoja, mitä siirtotien tekemiseen on mahdollista käyttää.

Käytännönosuudessa tutustutaan JP-Ravintolat Oy:n toimeksiannon mukaisiin tietojärjestelmien muutoksien toteutukseen käytännössä sekä toimenpiteisiin, joita toteutus vaati. Tähän kuuluu palvelimien asennus, tietoverkkojen muutos sekä uuden kassajärjestelmän käyttöönotto toimipaikassa.

Uuden kassajärjestelmän käyttöönotolla saavutettiin parempi hallittavuus tuotteiden, hintojen ja kanta-asiakasetujen hallinnassa sekä parannettiin toimipaikkakohtaisen raportoinnin tasoa. Verkkomuutoksella saavutettiin rahallista säästöä poistamalla verkoissa olleita päällekkäisyyksiä.

Asiasanat (avainsanat)

Tietoverkot, VPN, Tietojärjestelmät, Palvelimet

Sivumäärä	**Kieli**	**URN**
41	Suomi	

Huomautus (huomautukset liitteistä)

Ohjaavan opettajan nimi Koivisto, Matti	**Opinnäytetyön toimeksiantaja** X-Partner Mikkeli Oy

DESCRIPTION

MIKKELIN AMMATTIKORKEAKOULU Mikkeli University of Applied Sciences	**Date of the bachelor's thesis** 26 May 2011
Author(s) Tullinen, Lasse	**Degree programme and option** Information Technology

Name of the bachelor's thesis

Updating a company's network and POS system

Abstract

The purpose of this bachelor's thesis was to make changes to the company's information system commissioned by JP-Ravintolat Oy. These changes included updating the POS system, i.e. point of sale, and simplifying the two existing networks.

The theory part of this bachelor's thesis dealt with different technical solutions used in business world to join the data networks of companys' branch offices. This part also examined bridged and routed networks and virtual private networks (VPN). In addition, different mediums to join networks were also introduced.

The practical part introduced the changes which were made to the data system according to the requirements of JP-Ravintolat Oy. These changes include the installation of the servers, changes to the networks and the introduction of the new POS system.

Better manageability in products, product prices and regular customer discounts was achieved with the deployment of the new cash system and also the quality of reporting was enhanced. The network modification achieved reductions in costs by removing overlaps in the two networks.

Subject headings, (keywords)

Data networks, VPN, information system, servers,

Pages	**Language**	**URN**
41	Finnish	

Remarks, notes on appendices

Tutor	**Bachelor's thesis assigned by**
Koivisto, Matti	X-Partner Mikkeli Oy

SISÄLTÖ

1 JOHDANTO

Yrityksillä on hyvin erilaisia tarpeita liittyen tietotekniikkaan. Nämä tarpeet vaihtelevat yrityksen toimialasta, koosta ja palveluista riippuen. Varsinkin suurissa ja keskisuurissa ympäristöissä hyvin hoidettu ja hallittu tietotekniikka luo yritykselle säästöjä, mahdollistaa parempien palveluiden tuottamisen sekä helpottaa yrityksen jokapäiväistä toimintaa. Kuitenkin jossakin vaiheessa yrityksen tarpeet saattavat muuttua tai tekniikan kehittyessä tulee tarjolle kehittyneempää tekniikkaa, jolloin tulee ajankohtaiseksi päivittää yrityksen tietoteknisiä ratkaisuja. Viimeisten vuosien aikana kehitys onkin kulkenut kohti verkotettuja järjestelmiä, niissä yrityksen eri toimipisteissä olevat laitteet ja ohjelmistot liitetään toisiinsa tietoverkkojen avulla. Jos yritys pysyy mukana tässä kehityksessä, se tehostaa entisestään yrityksen toimintaa, palveluita ja kannattavuutta.

Tässä työssä tutustutaan erilaisiin verkkoratkaisuihin, joilla yhdistetään fyysisesti eri paikoissa sijaitsevien yrityksen eri toimipaikkojen verkot toisiinsa sekä millaisia tietoturvaratkaisuja tällaisissa verkoissa on käytettävissä.

Työn käytännön osassa toteutetaan JP-Ravintolat Oy:n toimeksiannon mukainen kassajärjestelmän päivitys uudempaan sekä olemassa olevien kahden tietoliikenneverkon muuttaminen yhdeksi helpommin hallittavaksi verkoksi. Verkkojen muuttamisella haetaan myös parempaa kustannustehokkuutta poistamalla kahden verkon aiheuttamia päällekkäisyyksiä.

Työn rakenne on seuraavanlainen. Ensinmäiseksi käsitellään erilaisia verkkoratkaisuja, joilla mahdollistetaan kahden, fyysisesti eri paikoissa sijaitsevien, esimerkiksi toimipisteiden tietoverkkojen yhdistäminen sekä tähän liittyvää tietoturvaa. Toiseksi esitellään yritys, jolle käytännönosassa tehtävä työ tehdään sekä nykyisiä käytössä olevia kassajärjestelmiä ja verkkoratkaisuja. Tämän jälkeen käydään läpi käytännön osiota, joka pitää sisällään kassajärjestelmän päivityksen sekä olemassa olevien kahden tietoverkon muuttamisen yhdeksi helpommin hallittavaksi kokonaisuudeksi. Muutossuunnitelma perustuu Micros-Fidelio Finland Oy:n tekemään suunnitelmaan, jonka käytännön toteutukseen osallistun.

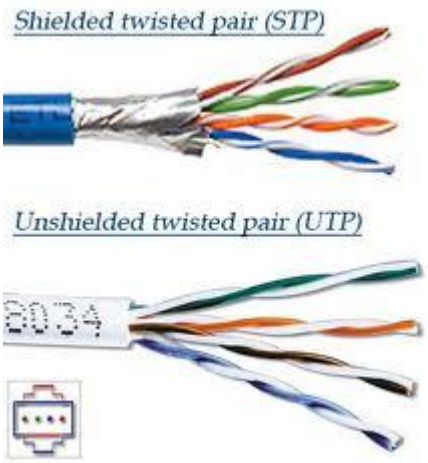
2 YRITYKSEN TIETOVERKKOJEN YHDISTÄMINEN

Yrityksen tietoverkkoja on mahdollista jatkaa ja liittää toisiinsa. Tämän mahdollistavat OSI-mallin eri kerroksilla toimivat sillat ja reitittimet. Mitä alhaisemmalla tasolla OSI-mallia käytössä oleva ratkaisu on, sen läpinäkyvämpää liikenne on. Tämä läpinäkyvyys taas mahdollistaa suuremman liikenteen läpäisykyvyn. [1, s. 255.]

Tässä luvussa käsitellään eri vaihtoehtoja, joilla mahdollistetaan fyysisesti eri paikoissa sijaitsevien yrityksen toimipaikkojen lähiverkkojen yhdistäminen toisiinsa. Yhdistävänä siirtotienä voi toimia esimerkiksi puhelinyhtiöltä vuokrattu kuparikaapeli, langaton WLAN-yhteys tai julkinen verkko eli internet. Edellä mainituissa esimerkeissä on omat hyvät ja huonot puolensa, joista seuraavassa tarkemmin.

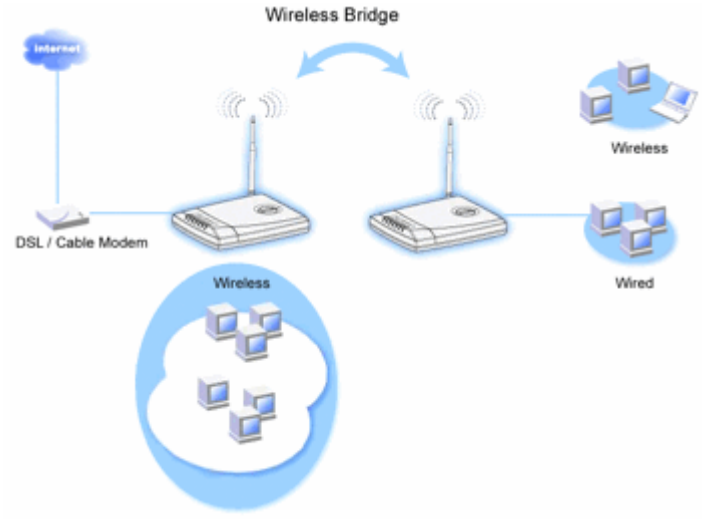
2.1 Siirtotie

Siirtotie, eli väylä, jolla kaksi etäverkkoa yhdistetään toisiinsa, on hyvin keskeisessä asemassa ajatellen kokonaisuuden toimivuutta. Tämä väylä voidaan toteuttaa usealla eri tavalla. Lyhyillä yhteysväleillä yleisin tapa liittää pisteet toisiinsa on käyttää kierrettyä parikaapelia TP (Twisted Pair). Kierretyssä parikaapelissa johtimet kierretään pariksi ja näin vähennetään ulkoisten sähkömagneettisten kenttien tuottamia häiriöitä siirrettävässä signaalissa. Tavallisen UTP-kaapelin (Unshielded Twisted Pair) lisäksi on olemassa STP- (Shielded Twisted Pair) ja FTP-kaapeleita (Folded Twisted Pair), joissa johdinparit on suojattu vielä ulkoisella metallivaipalla (kuva 1). Kierretyllä parikaapelilla toteutetaan yleensä lähiverkkojen kaapelointi, jolloin yhteyden maksimietäisyys on noin 100 metriä sekä muutaman kilometrin mittaiset yhteydet palveluntarjoajalta asiakkaan kotiin tai toimistoon. [2.]



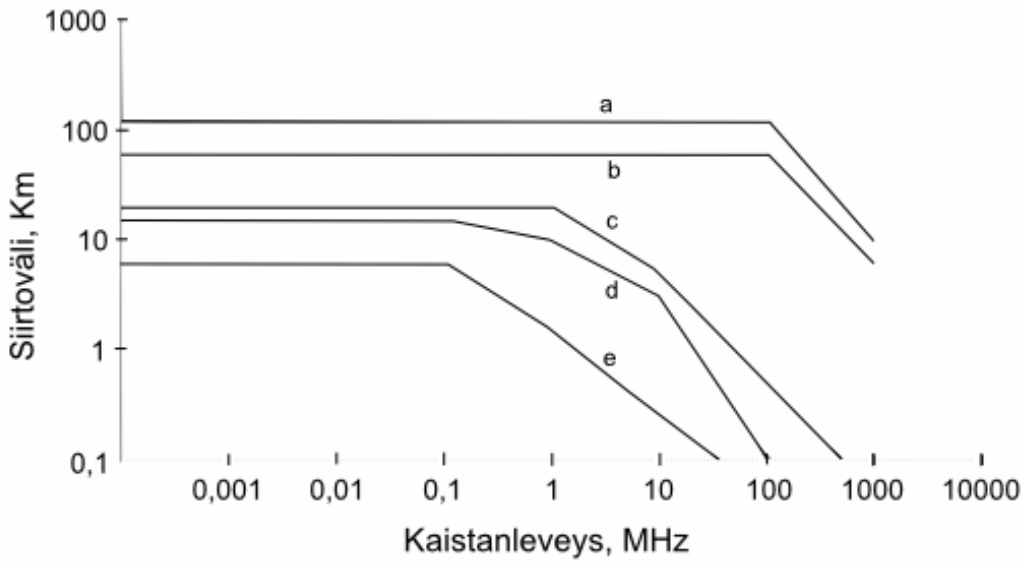
KUVA 1. STP ja UTP parikaapelit [3]

Lyhyillä etäisyyksillä voidaan käyttää myös langatonta siirtotietä paikoissa, joihin johtimen veto on syystä tai toisesta mahdotonta. Tällöin kahden WLAN tukiaseman välille muodostetaan sillattu yhteys, jonka kautta yhdistetään kaksi erillistä tietoverkkoa. Tällaisen sillatun yhteyden muodostaminen on mahdollista käyttäen esimerkiksi WDS:ää (Wireless Distribution System). WDS mahdollistaa tukiaseman käytön joko pääasemana (main base station), relay-asemana (relay base station) tai etäasemana (remote base station). Pääasema on usein liitetty langalliseen lähiverkkoon, josta on pääsy internetiin. Etäasemat muodostavat yhteyden pääasemaan joko relay-aseman kautta tai sitten suoraan (kuva 2). Relay-asemaa käytetään suurilla etäisyyksillä välittäjänä etäaseman ja pääaseman välillä. Langaton liikenne näiden asemien välillä on salattu joko käyttämällä WEP tai WPA salausta.[4.]



KUVA 2. WDS pääaseman ja etäaseman välinen yhteys [5]

Pidemmät yhteysvälit voidaan toteuttaa esimerkiksi valokuidulla. Valokuitu ei kärsi kuparikaapelin lailla suurista vaimennuksista tai ulkopuolisesta häiriöstä, joten kuituyhteyksillä päästään suurempiin etäisyyksiin kuin kuparikaapelilla (Kuva 3). Valon suuri taajuus mahdollistaa myös suuret tiedonsiirtonopeudet. [1,s. 103.]



a. Disperiosiirretty SM-kuitu
b. Standardi SM-kuitu
c. GK monimuotokuitu
d. koaksiaalikaapeli
c. Symmetrinen kaapeli

KUVA 3. Kuitu- ja kaapeliyhteyksien siirtoetäisyydet [6]

Valokuidut jaetaan kahteen ryhmään monimuoto- ja yksimuotokuitu. Monimuotokuidussa valo kulkee heijastumalla kuidun ytimen ja lasikuoren välillä ja sillä saavutetaan maksimissaan noin 2 km matka. Valon lähteenä voi olla käytössä joko laser tai led-valo ja kuidun paksuus on yleensä noin 62 mikrometriä. Monimuotokuitu voidaan valmistaa myös muovista, jolloin saadaan edullisia kuitukaapeleita, mutta yhteyden maksimi pituus on tällöin vain noin 200- 300 metriä. [6.]

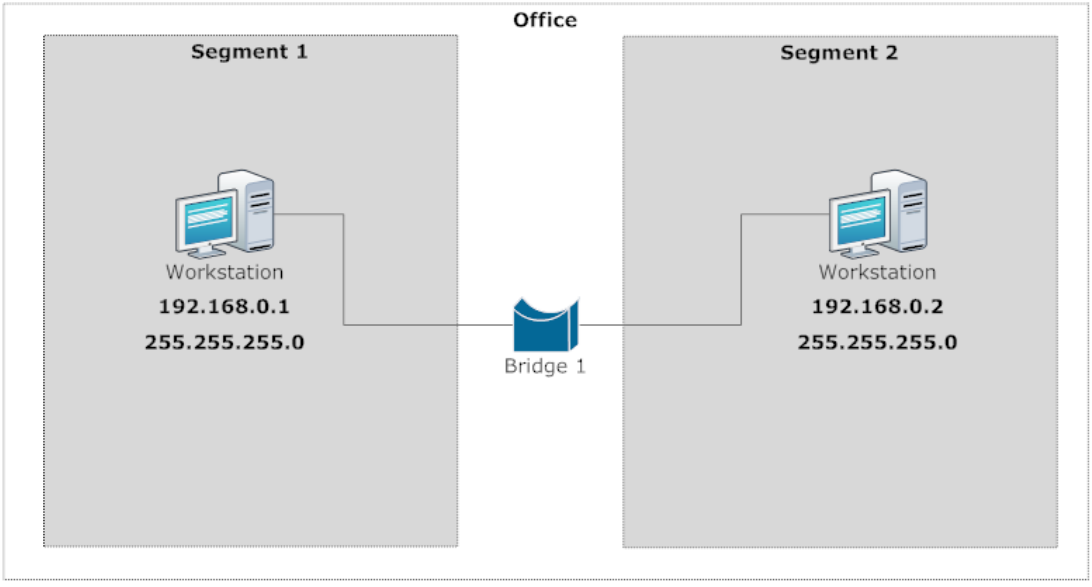
Yksimuotokuidussa valo kulkee halkaisijaltaan noin 5- 10 mikrometriä paksussa ytimessä. Ytimen halkaisija on niin pieni, että valon taittumista ei juuri tapahdu ja tästä johtuen yksimuotokuidussa tapahtuva vaimennus on huomattavasti pienempi kuin monimuotokuidussa. [7.]

Yksimuotokuidun pienestä halkaisijasta johtuen, se tarvitsee valonlähteekseen tietyllä aallonpituudella toimivan laserin. Tämä aallonpituus on normaalisti joko 1310 nm tai 1550 nm. [7.]

2.2 Sillatut yhteydet

Silta (bridge) on laite, jolla voidaan yhdistää kaksi erillistä verkkoa ja näin jatkaa olemassa olevan verkon fyysisiä mittoja tai jakaa yksi olemassa oleva verkko kahteen eri osaan. Se ei ota kantaa, mitä liikennettä sen kautta kulkee vaan se on protokolla riippumaton. Silta voi olla joko laitteisto- tai ohjelmistopohjainen. Sillatut verkot näkyvät käyttäjälle yhtenä verkkona. [1, s. 255.]

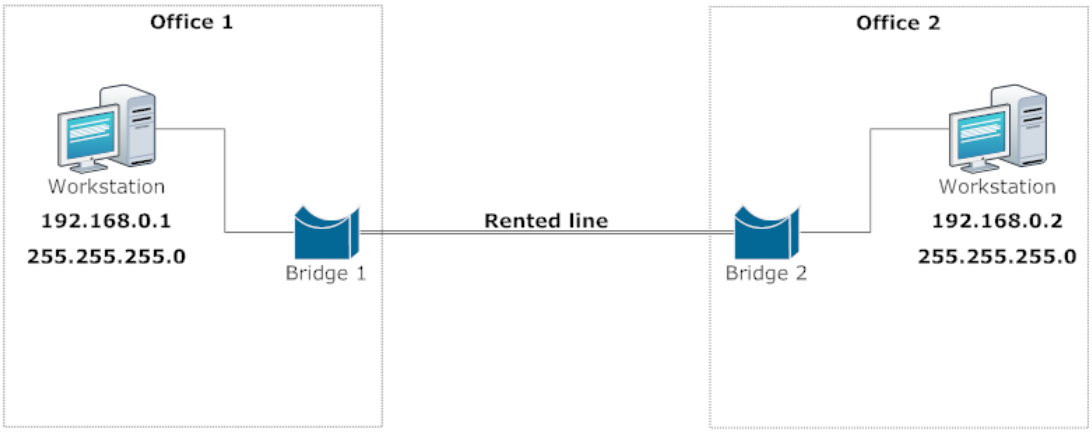
Jos siltausta käytetään olemassa olevan verkon jakamiseen, puhutaan paikallissillasta. Tällöin silta jakaa olemassa olevan verkon kahteen eri alueeseen eli segmenttiin (kuva 4). Segmentti on alue, jonka sisäistä liikennettä ei ohjata muihin segmentteihin. Ainoastaan jos eri segmenteissä sijaitsevilla laitteilla on liikennettä keskenään, ohjataan liikenne kyseisten segmenttien välillä. Tällä tavoin voidaan huomattavasti vähentää turhaa liikennettä verkon eri segmenteissä. [8, s. 84.]



KUVA 4. Paikallissilta

Jos siltausta käytetään kahden erillisen verkon yhdistämiseen eli jatkamaan olemassa olevan verkon fyysisiä mittoja, puhutaan etäsillasta. Tällöin tarvitaan kaksi siltaa, jot-

ka ovat yhdistettynä toisiinsa esimerkiksi kiinteällä yhteydellä, joka voi olla vaikka puhelinyhtiöltä vuokrattu kuparilinja, ja jossa käytetään jotakin kehystävää protokollaa esimerkiksi PPP (Point to Point. Protocol) (kuva 5.). [1,s. 256.]



KUVA 5. Etäsilta

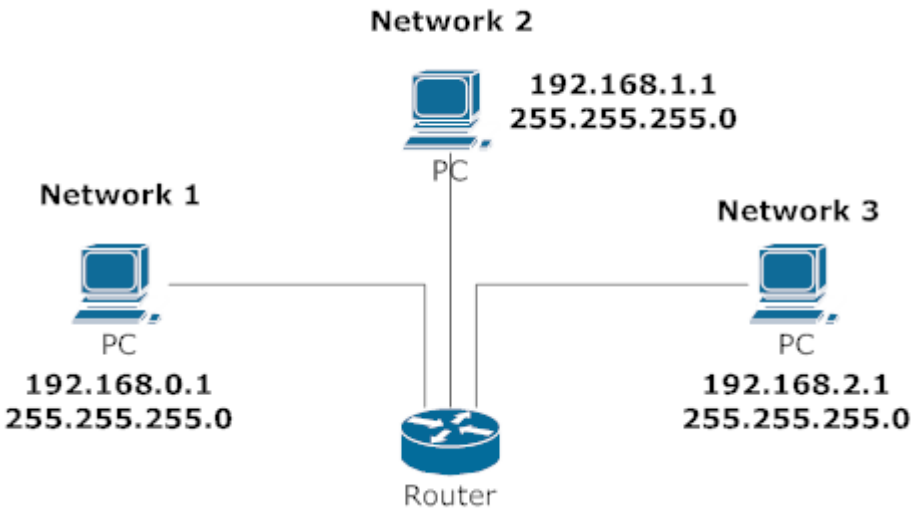
Siltayhteydet toimivat OSI-mallin siirtokerrostasolla (data link layer). Tämä tekee sillan toiminnasta nopeaa, koska sen ei tarvitse ottaa kantaa OSI-mallin ylempien tasojen sisältöön, vaan se voi nopeasti ohjata liikenteen eteenpäin. Silta onkin toiminnaltaan hyvin paljon kytkimen kaltainen. [9.]

Jotta silta tietäisi, missä segmentissä mikäkin laite sijaitsee, tarvitsee sen oppia verkossa sijaitsevien työasemien/laitteiden sijainti. Tutkimalla porttiin saapuvasta kehyksestä lähettäjän MAC-osoitteen ja tallentamalla muistiinsa sen sekä portin, johon kehys saapui, se muodostaa kuvan verkon rakenteesta ja verkossa olevien laitteiden sijainnista. [1, s. 254.]

Sillan etuina on sen mahdollistama läpinäkyvyys OSI-mallin siirtokerrostason yläpuolisille tasoille, verkon liikenteen hallittavuus eri segmenttien välillä sekä protokolla riippumattomuus. Huonoina puolina voidaan nähdä sillan huono skaalautuvuus suuriin verkkoihin, soveltumattomuus topologialtaan monimutkaisiin verkkoihin sekä se, että silta ei erottele yleislähetysalueita.

2.3 Reititinyhteydet

Kuten silta myös reititin (router) yhdistää verkkoja toisiinsa. Reititin tarjoaa kuitenkin monipuolisempaa verkon- sekä liikenteen hallintaa ja se soveltuukin siltaa paremmin suuriin verkkoihin. Reititin mahdollistaa myös tiettyjen turvallisuusmenetelmien käytön, joilla voidaan rajoittaa verkosta lähtevää tai saapuvaa liikennettä. Reititetyt verkot näkyvät käyttäjälle eri osoiteavaruuksina (kuva 6).



KUVA 6. Reititetyt verkot

Reititin toimii OSI-mallin verkkokerrostasolla (network layer) ja on siltaa monipuolisempi laite. Toisin kuin silta, reititin käyttää IP-osoitteita liikenteen ohjauksessa. Tämä mahdollistaa verkon aliverkottamisen, jolla saavutetaan verkon parempi hallinta. Lisäksi se vähentää verkossa tapahtuvaa yleislähetysliikennettä ja parantaa verkon suorituskykyä [10]. Reititin muodostaa verkontopologiasta, eli rakenteesta tarkan kuvan erinäisillä reititysprotokollilla, joilla se keskustelee muiden verkossa olevien reitittimien kanssa.

Reitittimellä voidaan myös sallia tai estää haluttu liikenne verkkojen välillä. Tällaiset säännöt voivat perustua esimerkiksi käytettävään protokollaan tai lähettäjän tai vastaanottajan IP-osoitteeseen.

Reitittimen etuina voidaan nähdä sen soveltuvuus topologialtaan monimutkaisiin verkkoihin, liikenteen hallittavuus eri verkkojen välillä, liikenteen hallittavuus protokollien avulla sekä yleislähetysalueiden erottelu.

2.4 VPN-yhteydet

Tietoverkkojen kehittyminen ja leviäminen miltei joka maailman kolkkaan on mahdollistanut fyysisesti toisistaan kaukanakin sijaitsevien verkkojen yhdistämisen käyttämällä hyväkseen julkista verkkoa, internetiä. Jotta tällainen liikenne olisi turvallista, on täytynyt kehittää tekniikka, jolla voidaan luotettavasti salata kahden päätepisteenvälinen liikenne. Tässä astuu kuvaan VPN (Virtual Private Network).

Alun perin VPN kehitettiin palvelemaan puhelinyhtiöiden tarpeita. Puhuttiinkin puhe-VPN:stä. Puhe-VPN mahdollisti yrityksen sisäisten lyhytnumeroiden käytön julkisilla numeroilla varustettujen toimitilojen välillä sekä selkeytti aikaisemmin monimutkaista laskutusta kaukopuheluissa. Lisäksi puhe-VPN mahdollisti palveluiden keskittämisen, kuten puheposti, yhden lyhytvalinta numeron alle. Näiden syiden takia puhe-VPN saavutti hurjan suosion yritysmaailmassa. Osa puhe-VPN:n peruskäsitteistä, kuten yksityisen osoitteen muodostus julkisenverkon välityksellä, helppokäyttöisyys ja skaalautuvuus siirrettiin puhetekniikasta datansiirtoon. [11, s. 30.]

Nykypäivänä VPN tarjoaa turvallisen tavan tietoverkkojen liittämiseen toisiinsa tai yksittäisten laitteiden liittämisen verkkoon, esimerkiksi etätyötä tekevän työntekijän kannettavatietokone. Jos VPN:ää käytetään kahden verkon yhdistämiseen, yhteys voidaan muodostaa kahden palomuurin väliin, mutta jos etätyöntekijä liittää koneensa yrityksen verkkoon, tarvitaan silloin jokin VPN-yhteyttä tarjoavan ohjelmiston asennus tietokoneelle.

2.4.1 VPN:n toiminta

VPN:ssä turvattu yhteys tehdään muodostamalla tunneloitu yhteys verkon päätepisteiden välillä. Tunnelointi itsessään ei vielä tarjoa tiedon salausta, vaan se ainoastaan kapseloi siirrettävän datapaketin jonkin toisen protokollan sisään. Salattuun yhteyteen tarvitaan vielä jokin protokolla salamaan liikenne. Näitä yleisessä käytössä olevia pro-

tokollia ovat IPSec (internet Protocol Security), L2TP (Layer 2 Tunneling Protocol) ja PPTP (Point To Point Protocol). [12.]

VPN:ssä tiedon salaus perustuu salausavainten käyttöön, mitä pidempi avain, sitä vaikeampi sillä tehty salaus on murtaa. Avain voi olla julkinen tai salainen. Salaisella avaimella tarkoitetaan VPN-osapuolten ennalta sopimaa avainta, jonka ainoastaan he tietävät. Samaa avainta käytetään tiedon salaamiseen sekä salauksen purkamiseen. Tällaisia yksityiseen avaimeen perustuvia salausjärjestelmiä ovat esimerkiksi DES (Data Encryption System), 3DES ja RC4 (Rivest Cipher4). Ongelmalliseksi salaisissa avaimissa muodostuu avainten hallinta, varsinkin jos käyttäjiä on paljon, kuinka koordinoida avainten vaihto. [11, s. 178.]

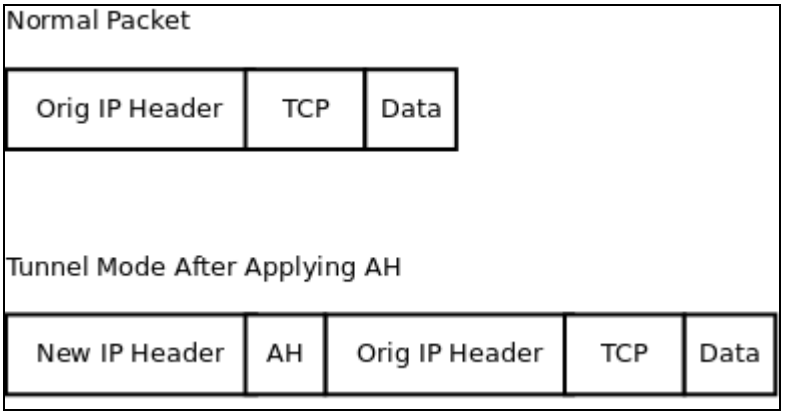
Julkiseen avaimeen perustuva salaus, Diffie-Hellman avaimenvaihtoprotokolla koostuu oikeastaan kahdesta avaimesta, yksityisestä avaimesta ja siitä matemaattisesti lasketusta julkisesta avaimesta. Tällä kaikkien saatavilla olevalla julkisella avaimella salatun viestin purkaminen onnistuu vain samaa alkuperää olevalla yksityisellä avaimella. Eli ainoastaan se kenen julkisella avaimella viesti on salattu voi myös purkaa sen. Tällaiset julkisen avaimen algoritmit ovat suhteellisen raskaita laskea, niinpä niitä käytetäänkin usein ”digitaalisena kirjekuorena” salaisen avaimen vaihdossa. Tällöin varsinainen liikenteen salaaminen tapahtuu kevyemmällä salaisella avaimella.[11, s. 178.]

VPN tarjoaa myös käyttäjien ja tiedon todentamisen. Näillä varmistetaan, että linjan päissä ovat ne henkilöt tai laitteet, mitkä siellä kuuluisikin olla ja, että tieto on säilynyt muuttumattomana. Käyttäjän todentamisessa voidaan käyttää paikallisia staattisia salasanoja, kolmannen osapuolen varmistamia sertifikaatteja tai julkiseen avaimeen perustuvaa salausta. Tiedon todentamisella tarkoitetaan, että vastaanottaja saa tiedon muuttumattomana, eikä siirrettävä tieto ole päässyt muuttumaan siirtovälillä vahingossa tai tahallisesti. [13.]

2.4.2 IPSec

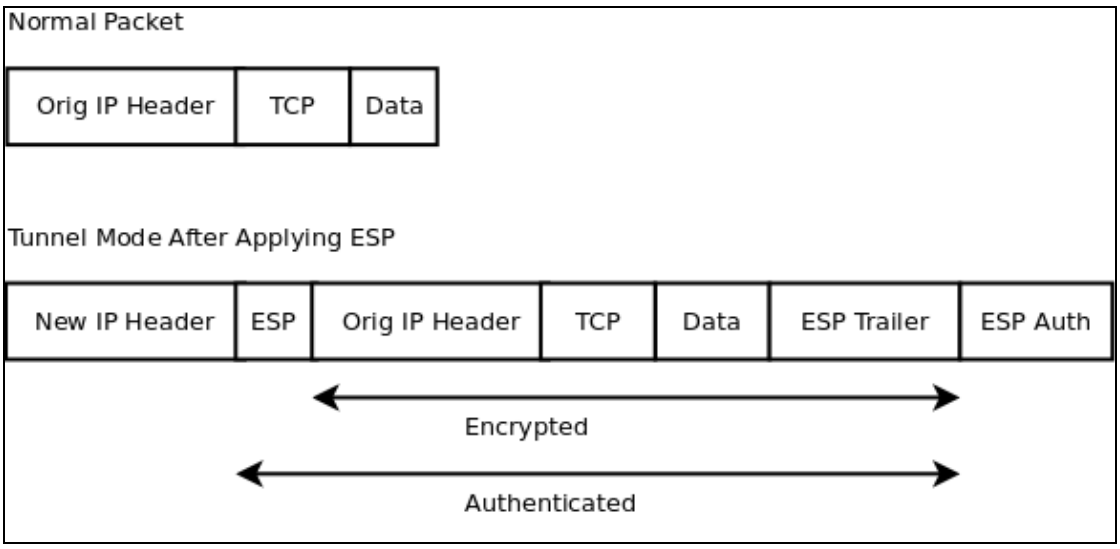
IPSec on kokoelma eri protokollia ja algoritmeja, joilla varmistetaan turvallinen tiedonsiirto. Käytetyt protokollat tarjoavat salauksen, osapuolten todennuksen sekä tiedon eheyden varmistamisen. [14, s. 325-326.]

IPSec:ssä käytetyt kaksi yleisintä protokollaa ovat AH (Authentication Header) sekä ESP (Encapsulated Security Payload). AH nimensä mukaisesti vain todentaa käyttäjät, joiden välillä tiedonsiirto tapahtuu sekä varmistaa tiedon muuttumattomuus siirtovälillä. Se ei tarjoa varsinaista salausta siirrettävälle datalle, vaan se kapseloi IP-paketin ja muodostaa sen otsikkotiedoista sekä dataosiosta tarkistuskoodin (kuva 7). Tämä koodi tehdään käyttäen salaista avainta, jonka vain lähettäjä ja vastaanottaja tietävät. IP-paketin otsikkotiedoista löytyvät mm. lähettäjän ja vastaanottajan IP-osoitteet. [14, s. 328-329.]



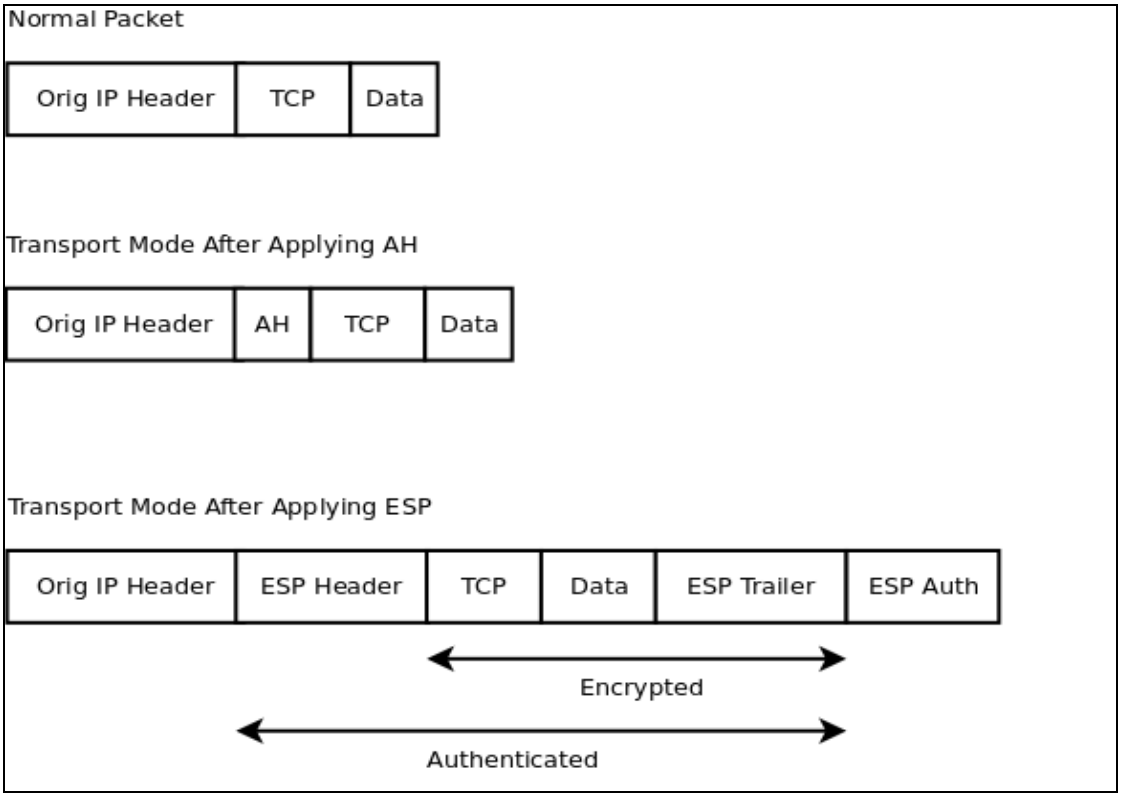
KUVA 7. Normaali ja AH tunneloitu paketti [15]

ESP tarjoaa AH:sta poiketen myös tiedonsalauksen. Samalla tavoin kuin AH, myös ESP kapseloi siirrettävän IP-paketin sisäänsä muodostaen uuden IP-paketin, kuitenkin niin, että alkuperäinen IP-paketti on salattu (kuva 8). Salaus tehdään käyttämällä salattua avainta. ESP mahdollistaa autentikoidun ja salatun yhteyden muodostamisen kahden pisteen välille.



KUVA 8. Normaali ja ESP tunneloitu paketti [15]

Niin AH kuin ESP on mahdollista ajaa tunnel mode:n lisäksi niin sanotussa transport mode:ssa. Tällöin siirrettävää IP-pakettia ei kapseloida siirtoprotokollan sisään, vaan AH tai ESP luo omat otsikkotietonsa alkuperäisen IP-otsikkotiedon ja ULP:n (Upper Layer Protocol) väliin (kuva 9). Eli pelkkä siirrettävä data autentikoidaan tai salataan. Yhteys ei tällöin ole tunneloitu. Tällaista yhteyttä käytetään yleensä host-to-host välisissä yhteyksissä. [15.]



KUVA 9. AH ja ESP transport mode [15]

2.4.3 PPTP

PPTP kehitettiin alun perin Microsoftin, ECI/Telematicsin, Ascend Communications sekä US Roboticsin toimesta ja se oli ensimmäinen protokolla, joka tarjosi virtuaalisten yksityisverkkojen muodostamisen julkisen verkon ylitse Microsoftin käyttöjärjestelmissä. Microsoftin mukana olo mahdollisti näin protokollan käyttöönotolle laajan levikin ja siitä tulikin suosittu erityisesti yritysmaailmassa, yritysten huomattua tällaisen teknologian tuomat edut kuten esimerkiksi etätyöskentely. [11, s. 114-115.]

PPTP:ssä on mahdollista käyttää useita protokollia tiedon salaamiseen sekä käyttäjien autentikointiin, aivan kuten IPSec:ssä. Koska PPTP on jatke PPP:lle, se tarjoaa samat autentikointimetodit kuin PPP.

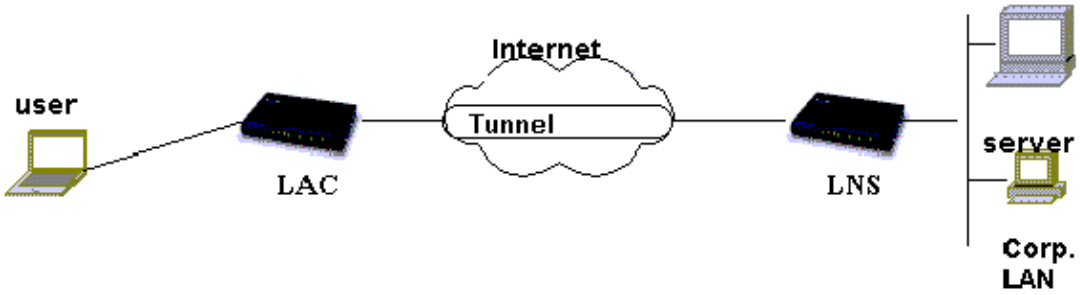
PPTP:ssä on käytössä kaksi pakettien perustyyppiä, datapaketti ja valvontapaketti. Datapaketit sisältävät varsinaisen siirrettävän tiedon ja ne on kapseloitu käyttäen GRE-protokollaa (Generic Routing Protocol). Valvontapaketteja käytetään merkinantoon sekä tilantiedusteluun ja ne kulkevat TPC-istunnon välityksellä. Jotta asiakas voisi muodostaa PPTP-tunnelin, täytyy hänen ensiksi muodostaa TCP-istunto palvelimen kanssa. Tämän jälkeen PPTP-valvontaviestit voivat kulkea palvelimen ja asiakkaan välillä. Näillä valvontaviesteillä muodostetaan, hallitaan ja päätetään tunnelin toiminta. Kun tunneli on saatu muodostettua, voivat GRE-kapseloidut datapaketit kulkea asiakkaan ja palvelimen välille muodostetun tunnelin kautta. Istunnon lopettaakseen asiakas lähettää palvelimelle valvontapaketin, joka lopettaa istunnon ja purkaa tunnelin.[11, s. 116.]

PPTP:n kehitys on nykyisin pysähtynyt, koska sen on korvannut L2TP -protokolla ja kiinnostus on siirtynyt kohti IPSec- ja SSL -protokollilla toteutettuja VPN-yhteyksiä. [22.]

2.4.4 L2TP

L2TP on jatke PPP-protokollalle, sekään ei itsessään tarjoa yhteyden salausta, vaan siihen se käyttää erinäisiä salausprotokollia. Se yhdistää Microsoftin luoman PPTP:n sekä Ciscon tekemän L2F (Layer 2 Forwarding) protokollien parhaat puolet luodessaan tunneloidun yhteyden. [16.]

L2TP -tunneli muodostuu sen päätepisteissä sijaitsevien LAC (L2TP Access Concentrator) ja LNS (L2TP Network Server) välille. LAC on laite, johon asiakas kytkeytyy ja, joka muodostaa tunneloidun yhteyden sen ja LNS:n välille (kuva 10). L2TP yksilöi yhteydet session ID:llä, joten on mahdollista muodostaa useita virtuaalisia verkkoja saman tunneloidun yhteyden kautta. [17.]

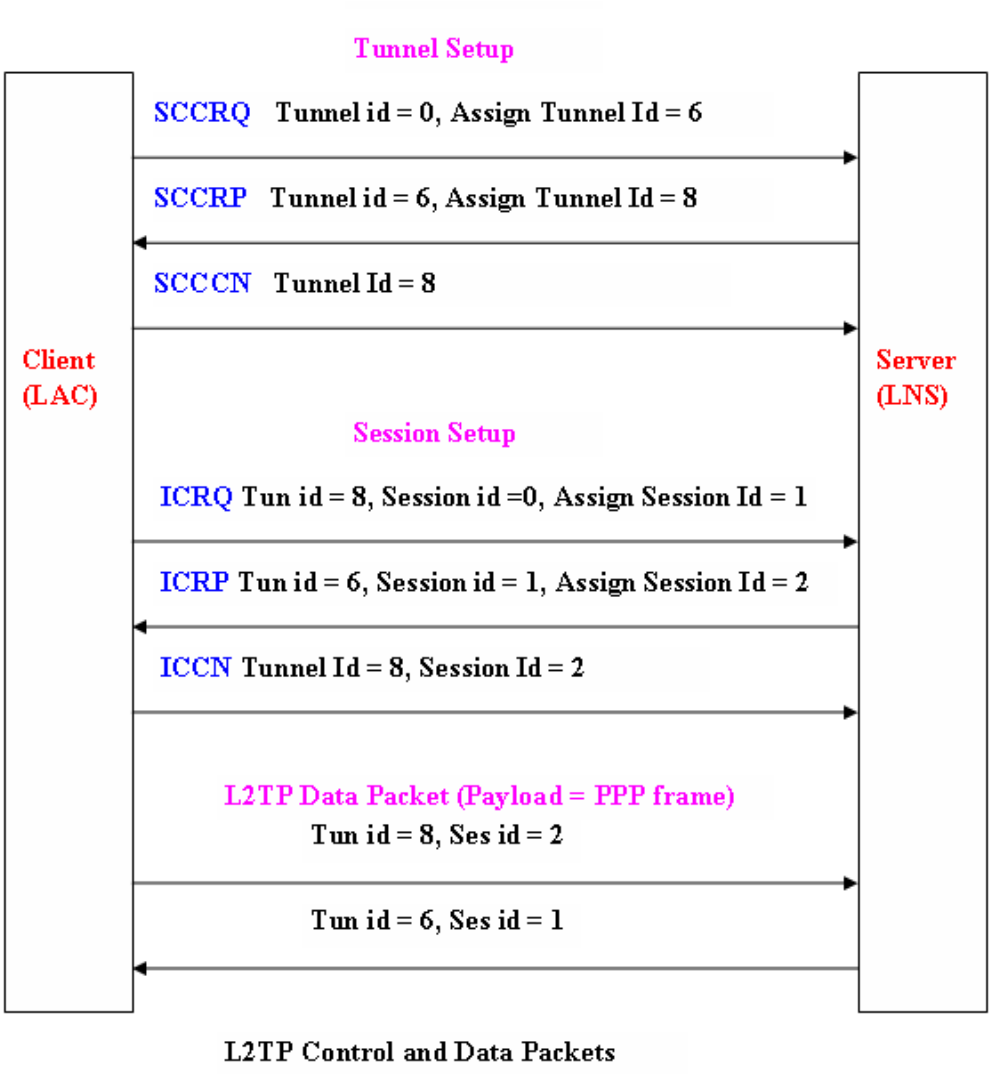


KUVA 10. L2TP tunneli [18]

Kaikki L2TP:n lähettämät paketit ovat UDP-kapseloituja eli L2TP muodostaa niin sanotun yhteydettömän yhteyden. Tämän vuoksi L2TP joutuu käyttämään enemmän komento- ja valvontapaketteja kuin esimerkiksi PPTP, jonka käyttämään TCP-protokollaan on sisään rakennettu useita erilaisia valvonta toimintoja. [11, s. 129.]

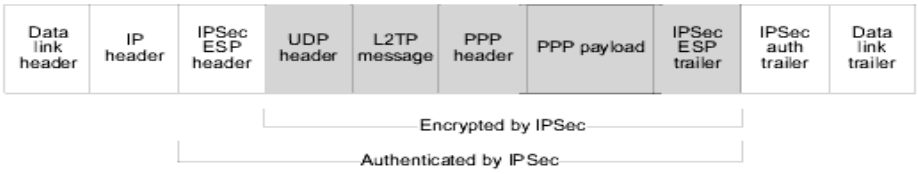
TCP-protokolla muodostaa valvotun yhteyden eli ns. yhteydellisen yhteyden. Tämä yhteys muodostetaan päätepisteiden välille ja tällä yhteysvälillä liikkuvat paketit kuitataan lähettäjälle vastaanotetuiksi. Jos lähettäjä ei saa tietyn ajan sisällä kuittausta vastaanotosta, lähettää se saman paketin uudestaan. TCP-protokolla huolehtii myös yhteyden lopettamisesta hallitusti. Yhteys on mahdollista lopettaa niin asiakkaan kuin palvelimen toimesta. [19.]

Koska L2TP ei käytä TCP-protokollaa, se tarvitsee yhteyden muodostamiseen useita komento- ja valvontapaketteja. Näillä paketeilla määritellään kummallekin yhteyden osapuolelle, asiakkaalle ja palvelimelle, tunnel id sekä session id, joita käytetään yhteyden ja tunnelin muodostamisen jälkeen datapakettien lähettämiseen ja vastaanottoon (kuva 11). [17.]



KUVA 11. L2TP yhteyden muodostaminen [17]

L2TP:tä on mahdollista käyttää myös esimerkiksi IPSec:n kanssa. Tällöin L2TP-paketit kapseloidaan IPSec:n sisään (kuva 12). Tällä mahdollistetaan esimerkiksi käyttäjän ja laitteen autentikointi sekä parempi tietoturva siirtovälille. [20.]



KUVA 12. L2TP ja IPSec [21]

2.4.5 SSL VPN

SSL VPN (Secure Socket Layer Virtual Private Network) mahdollistaa VPN-yhteyden muodostamisen nykyaikaisen WWW-selaimen kautta. Käyttäjän ei tarvitse asentaa erillisiä VPN-ohjelmia tietokoneelleen, vaan yhteyden luominen tapahtuu helposti ja vaivattomasti käyttäen WWW-selaimeen sisäänrakennettuja toimintoja hyväksi. [23.]

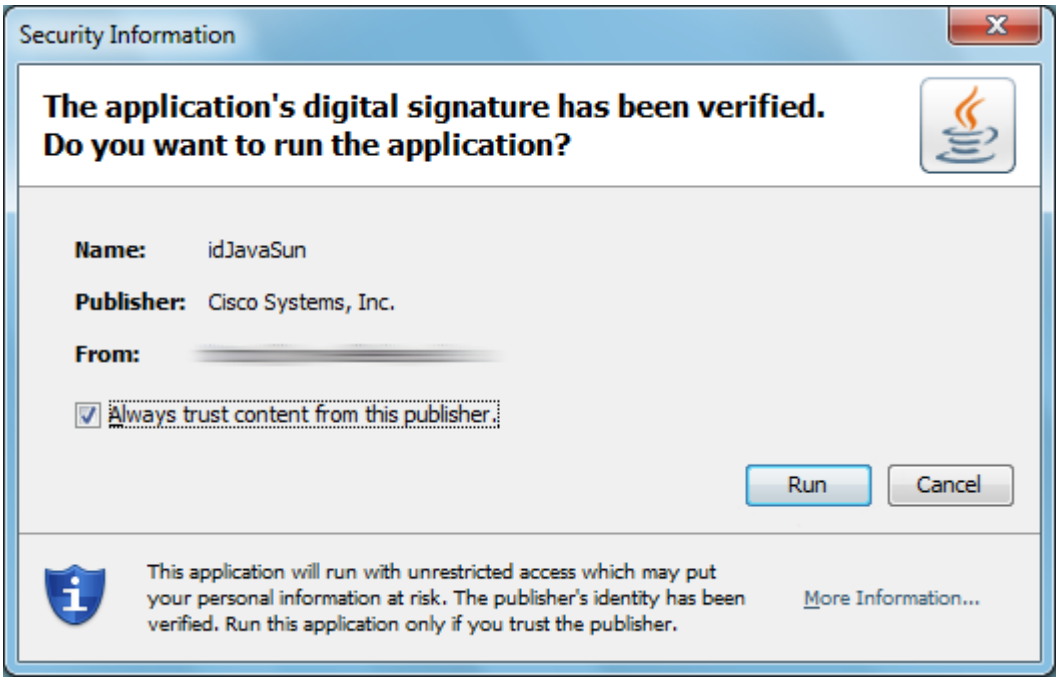
SSL VPN käyttää liikenteen salaamiseen SSL-protokollaa tai sen seuraajaa TLS- protokollaa (Transport Layer Security). Alun perin SSL kehitettiin Netscape Corporation:n toimesta salaamaan http-yhteyksiä eli www-sivujen suojaamiseen. Koska SSL ei ole rajoitettu pelkästään HTTP-protokollaan, sitä käytetään nykyisin useissa eri sovelluksissa alkuperäisen tarkoituksensa lisäksi, muun muassa sähköposti-, VoIP- (Voice over IP) sekä pikaviestiohjelmien yhteyksien salaamiseen. [24.]

Kaksi SSL VPN:n päätyyppiä ovat SSL portal VPN ja SSL tunnel VPN. SSL portal VPN mahdollistaa salatun yhteyden muodostamisen WWW-sivuun, portaaliin, josta käyttäjä voi suorittaa ja käyttää useita erilaisia palveluita tai resursseja, kuten etätyöpöytäyhteys, tiedostojen jako tai verkkosovellusten käyttö (kuva 13). [25.]

KUVA 13. SSL VPN portaali [25]

SSL tunnel VPN -yhteys muodostetaan myös web-sivun kautta, tällöin selaimen täytyy tukea active content -ympäristöä eli esimerkiksi Javaa, ActiveX:ä tai Flash:a. Selain asentaa kirjautumisen yhteydessä, esimerkiksi Java-ohjelmapaketin, joka luo virtuaalisen verkkosovittimen, minkä kautta sillattu yhteys muodostetaan kohdeverkkoon

(kuva 14). Yhteys on tämän jälkeen auki niin kauan kuin selainta ei suljeta tai muuten katkaista yhteyttä. Yhteyden ollessa auki, käyttäjän on mahdollista käyttää kohdeverkon resursseja. [26.]



KUVA 14. Java SSL VPN [27]

SSL VPN:ssä on myös heikkoutensa. Koska SSL VPN on käyttäjän kannalta tehty erittäin helpoksi ja yhteyden luominen on mahdollista melkein miltä koneelta tahansa, saattaa käytettäessä julkisia tietokoneita ongelmaksi muodostua kolmannen osapuolen luomat ohjelmistot, kuten esimerkiksi Google Desktop. Se tallentaa välimuistiinsa vieraillut nettisivut ja tällöin tallentuu myös SSL VPN yhteyden muodostamiseen käytetty sivu sekä mahdollisesti muuta tietoa yhteyden luomisesta. Google Desktopin kaltaiset ohjelmat mahdollistavat yhteyden väärinkäytön varsinkin, jos yhteyden muodostamiseen on käytetty julkista tietokonetta. Julkisten tietokoneiden käyttö asettaa yrityksen tietokoneet alttiiksi myös viruksille. [26.]

3 TOIMEKSIANTO

Suoritin opinnäytetyön käytännönosion ollessani työharjoittelussa X-partner Mikkeli Oy:ssä. Työn toimeksiantaja oli JP-Ravintolat Oy ja toimeksianto koski yrityksen tietoverkkojen yksinkertaistamista ja kassajärjestelmien päivittämistä uudempaan versioon. Työ suoritettiin yhteistyössä kassajärjestelmän toimittajan, Micros-Fidelia Oy:n kanssa, jolta myös alkuperäinen suunnitelma kassajärjestelmän muutokselle sekä verkon rakenteen muutokselle oli tullut.

X-Partner Mikkeli Oy:n päätoimiala on toimisto- laitteiden ja tarvikkeiden myynti. Tämän lisäksi yritys tarjoaa asiakkailleen tietojärjestelmien ylläpitoa, johon kuuluu muun muassa tietoverkkojen, palvelinten ja työasemien ylläpito. Yrityksen päätoimipaikka sijaitsee Kuopiossa.

Micros-Fidelia Oy on yritys, joka kehittää ja tarjoaa asiakkailleen ohjelmisto ja laiteratkaisuja. Sillä on toimintaa yli 140 maassa ja Suomessa se toimii nimellä Micros-Fidelio Finland Oy.

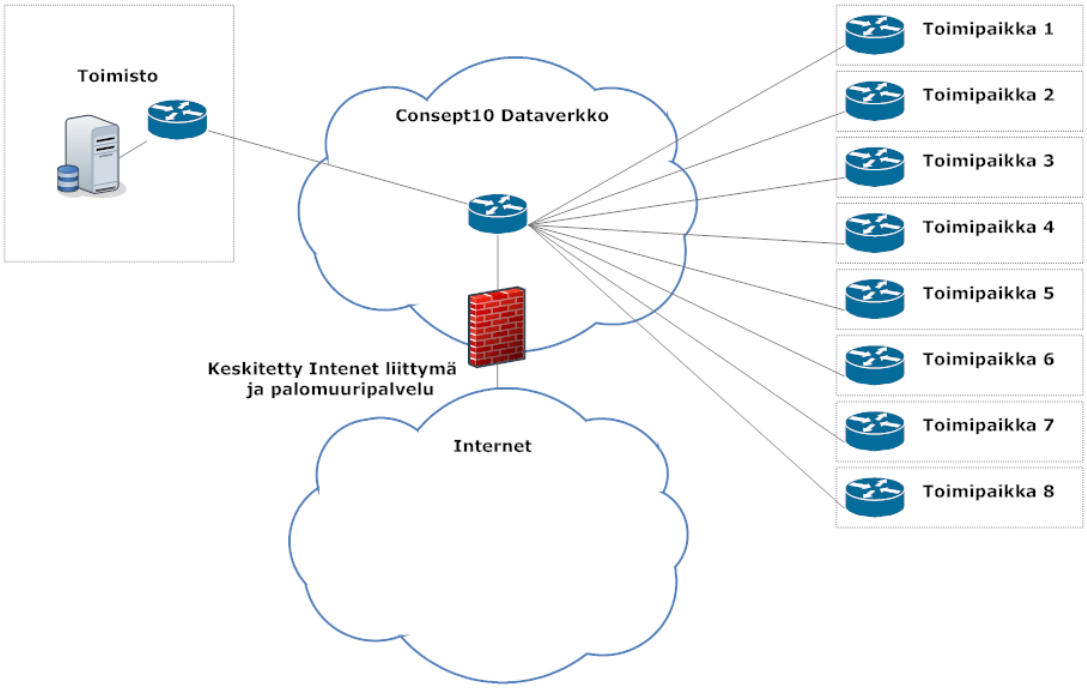
JP-Ravintolat Oy on mikkeliläinen yritys, joka on keskittynyt yö- ja ravintolatoimintaan. Yrityksellä on useita toimipisteitä Mikkelin keskustan alueella sekä muutama toimipiste hieman kauempana keskustasta.

3.1 Lähtötilanne

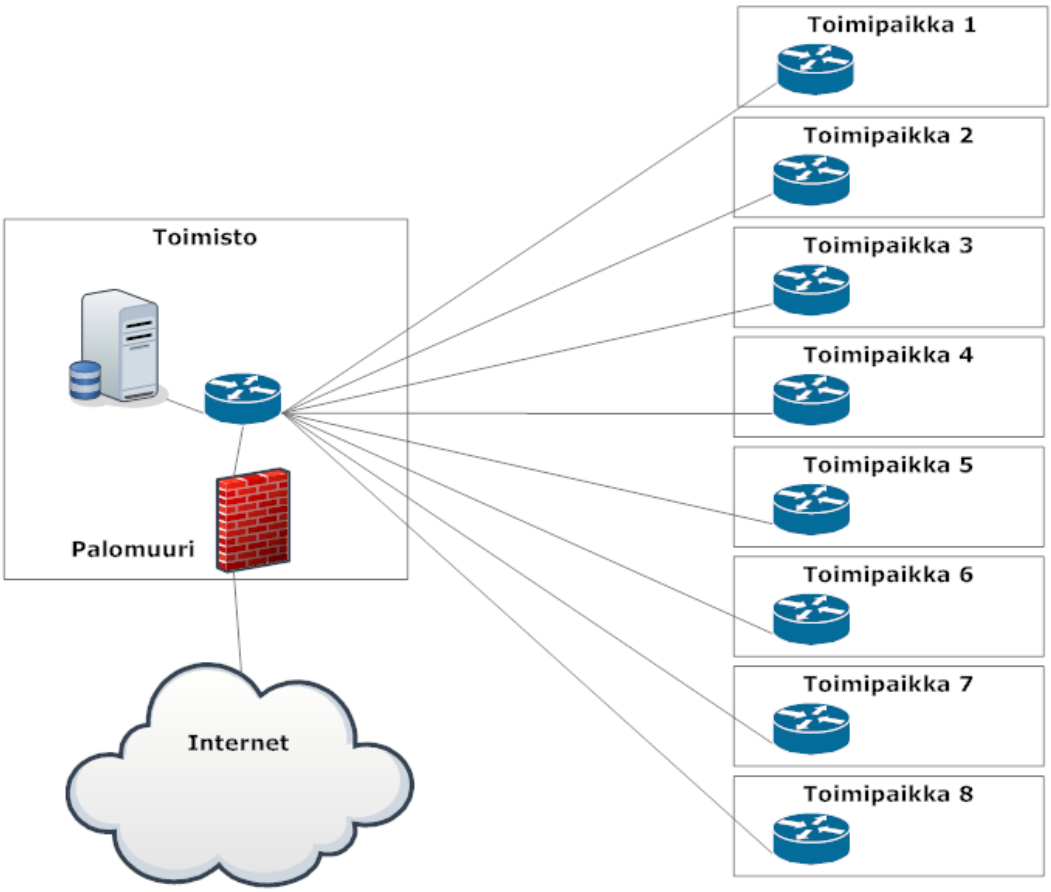
JP-Ravintolat Oy:llä on käytössään Microksen tuottama kassajärjestelmä, jonka palvelin sijaitsee yrityksen toimistolla ja josta käsin se palvelee keskitetysti yrityksen kaikkia toimipisteitä. Koska tätä kassajärjestelmää ei ole tarkoitettu näin laajan toimipisteverkoston ylläpitoon ja kaikki ravintolat toimivat hieman erilaisella periaatteella, on siitä aiheutunut ongelmia muun muassa tuotteiden, hintojen ja kanta-asiakasetujen hallintaan. Käytössä oleva kassajärjestelmä vaatii toimiakseen myös oman erillisen tietoverkon toimipisteiden ja yrityksen toimiston välille, sillä kassajärjestelmän palvelin sijaitsee toimistolla. Tämä tietoverkko on Consept10:n toimittama lähiverkkoratkaisu (kuva 15) ja se yhdistää toimipaikkojen kassat yrityksen kassaverkkoon. Tämän Consept10-lähiverkon lisäksi yrityksellä on käytössään toimipisteiden ja toimiston välille rakennettu lähiverkko, jolla hoidetaan toimipaikkojen työasemien liittäminen

yrityksen sisäverkkoon. Lähiverkko käyttää SHDSL-yhteyksiä Consept10:ltä vuokrattujen kuparilinjojen ylitse (kuva 16). Näiden kahden verkon lisäksi osassa yrityksen toimipaikoista on käytössä ADSL-liittymät asiakaskäyttöä varten.

Palvelimia yrityksellä on kaksi kappaletta, joista toinen on kassajärjestelmäpalvelin ja toinen palvelin toimii domain controller:na sekä palvelee yrityksen omia tarpeita.



KUVA 15. Consept10 lähiverkkoratkaisu



KUVA 16. SHDSL yhteyksillä toteutettu verkko

3.2 Tavoitteet

Tavoitteet tälle työlle ovat seuraavat. Korvata vanha kassajärjestelmä uudella päivitetyllä versiolla, joka vastaa paremmin yrityksen tarpeita. Tällöin jokaisessa toimipaikassa toimisi itsenäinen kassajärjestelmä, jota kuitenkin hallittaisiin keskitetysti yhdestä paikasta. Tällä helpotetaan ravintolakohtaisten tuotteiden, hintojen ja kanta-asiakasetujen hallintaa sekä parannetaan raportoinnin tasoa ja tarkkuutta.

Tavoitteena on myös muuttaa yrityksen verkon rakennetta siten, että käytössä oleva Concept10:n lähiverkkoratkaisu jäisi kokonaan pois ja sen toiminta korvattaisiin olemassa olevalla SHDSL-yhteyksillä toteutetulla verkolla. Mahdollisesti myös toimipaikkakohtaiset ADSL-liittymät poistuisivat käytöstä ja asiakaskäyttöön tarkoitetun verkon liikenne ohjattaisiin tämän SHDSL-verkon kautta toimistolle ja sieltä edelleen internetiin. Näillä muutoksilla saavutettaisiin säästöjä kuluissa, poistamalla turhia päällekkäisyyksiä olemassa olevista verkoista.

Uudistus korvaa myös olemassa olevat kaksi palvelinta yhdellä uudella palvelimella, joka tulisi palvelemaan uutta kassajärjestelmää sekä yrityksen omia tarpeita.

3.3 Vastuualueet

Microksen vastuulla on kassajärjestelmän asennus pääpalvelimelle, johon on esiasennettu Microsoft Windows Server 2003 sekä yhdelle toimipaikkapalvelimelle, johon on esiasennettu Microsoft Windows XP. Tämän lisäksi Micros vastaa henkilökunnan koulutuksesta, auttaa tietokantojen siirrossa sekä ensimmäisen toimipaikan liittämisessä uuteen järjestelmään. Ensimmäisen toimipaikan liittämisen jälkeen Micros testaa sekä seuraa järjestelmän toimintaa seuraavien kahden viikon ajan ja puuttuu mahdollisiin epäkohtiin, joita saattaa ilmetä järjestelmän toiminnassa.

JP-Ravintolat Oy:n vastuulla on vanhojen tietokantojen siirto ja niihin tarvittavien rakennemuutosten teko siirryttäessä uuteen järjestelmään.

X-Partner Mikkeli Oy:n vastuulla on tarvittavien palvelimien ja toimipaikkapalvelimien toimittaminen ja niihin liittyvien käyttöjärjestelmien sekä oheisohjelmien asennus että tiedostojen varmentaminen asentamalla kullekin koneelle RAID1 levynpeilauksen. Toimipaikkapalvelimien asennuksesta on sovittu niin, että Microksen asennettua kassajärjestelmä ensimmäiselle toimipaikkapalvelimelle, siitä otetaan levykuva, jolla se asennetaan muihin toimipaikkapalvelimiin. Näin saadaan vähällä vaivalla asennettua niin käyttöjärjestelmä kuin kassajärjestelmäkin muihin toimipaikkapalvelimiin. Lisäksi X-Partner vastaa nykyisten verkkojen muuttamisesta yhdeksi sekä muutoksesta johtuvien konfiguraatioden tekemisestä yrityksen työasemiin, maksupäätteisiin ja verkkolaitteisiin.

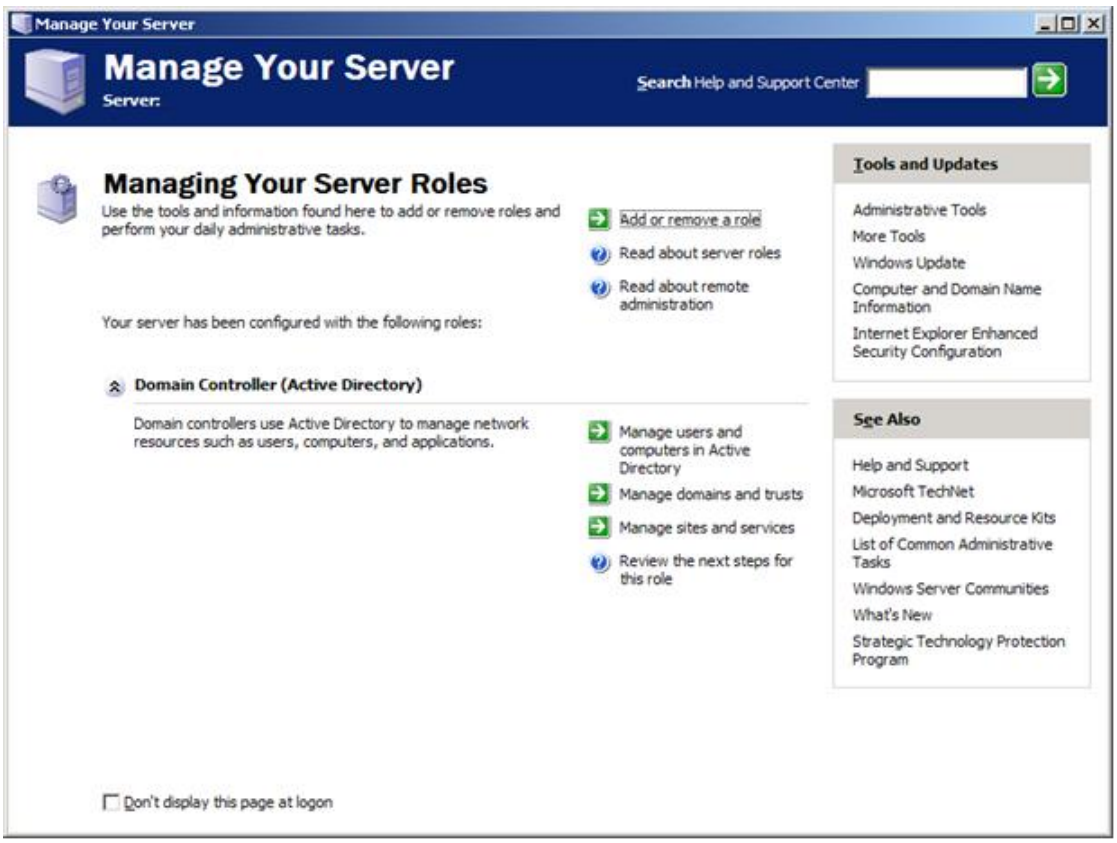
4 TOTEUTUS

Työn alustavasta etenemisjärjestyksestä sovittiin seuraavasti. Ensimmäisenä X-Partner Mikkeli Oy hankkii tarvittavan laitteiston, sekä tekee niihin tarvittavat asennus- ja muutostyöt. Tähän kuuluu lähinnä toimipaikkapalvelimien ja pääpalvelimen käyttöjärjestelmien asennus ja lisäkiintolevyjen asennus koneisiin. Tämän jälkeen Micros asentaa kassajärjestelmän yhdelle toimipaikkapalvelimelle sekä pääpalvelimelle, jonka jälkeen X-Partner Mikkeli Oy hoitaa toimipaikkapalvelimien kloonauksen. Tällä välin Micros kouluttaa JP-Ravintolat Oy:n henkilöstöä uuden järjestelmän käytössä sekä käyttöönotossa. Koulutuksen jälkeen JP:n henkilöstö tekee tietokantojen siirron uuteen järjestelmään. Kun tarvittavat tietokannat on saatu tehtyä pääpalvelimelle, voidaan ensimmäisen toimipaikan käyttöönotto aloittaa. Tällöin tehdään toimipaikan verkkoon tarvittavat muutokset sekä toimipaikanpalvelimelle tarvittavat jälkiasennukset. Näiden toimien jälkeen liitetään toimipaikan kassalaitteet uuteen järjestelmään, jonka jälkeen toimipaikka on valmis.

Ensimmäisen toimipaikan liittämisen jälkeen järjestelmää testataan seuraavan kahden viikon ajan. Jos suurempia ongelmia ei ole ollut, liitetään muutkin toimipaikat yksikerrallaan uuteen järjestelmään. Kun viimeinenkin toimipaikka on saatu liitettyä, voidaan sanoa irti sopimus Concept10:n lähiverkkoratkaisun osalta ja tämän jälkeen työ on osaltani valmis.

4.1 Palvelinten asennus

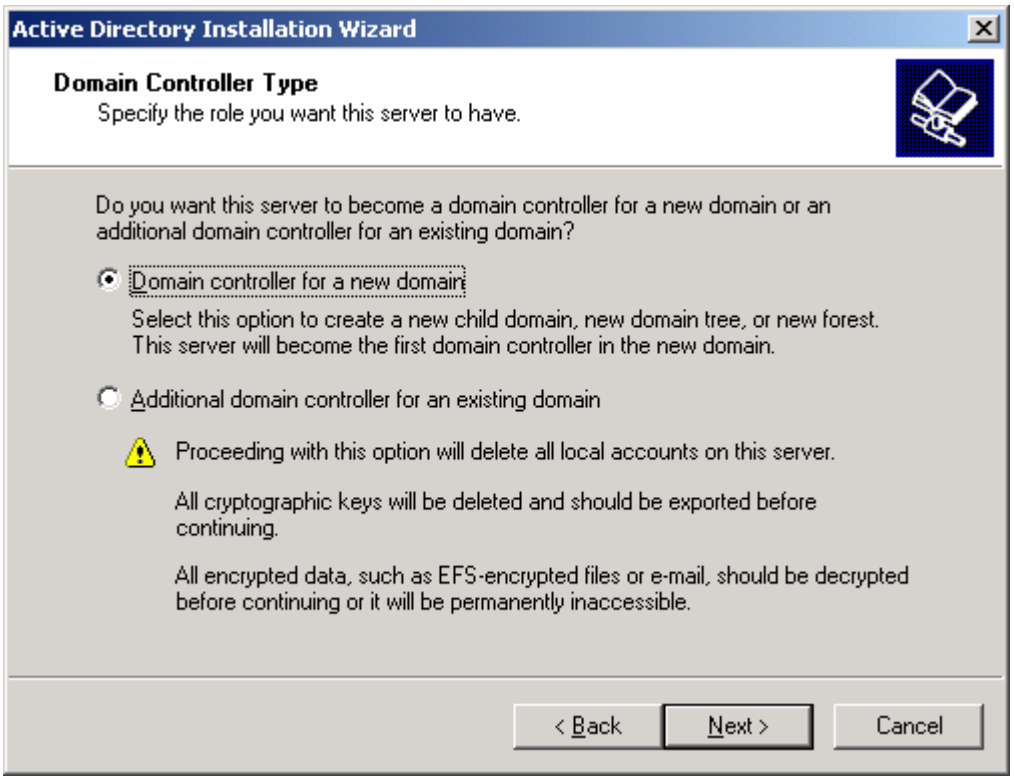
Työn ensimmäinen vaihe osaltani oli pääpalvelimen sekä yhden toimipaikkapalvelimen käyttöjärjestelmien asentaminen. Pääpalvelimelle asennettiin Microsoft Windows Server 2003. Rooleiksi palvelimelle asennettiin Domain Controller, Print Server, DNS Server sekä File Server. Roolit asennettiin käyttäen palvelimen hallinnasta löytyvällä ohjatulla asennuksella (kuva 17).



KUVA 17. Roolien ohjattu asennus

Domain Controller on rooli, jolla hallitaan keskitetysti toimialueeseen liitettyjen käyttäjien oikeuksia, kirjautumisia yms. sekä se ylläpidetään tietokantaa toimialueen resursseista [28]. Tämä antaa järjestelmänvalvojalle keinon määrittää eri käyttäjille tiettyjä oikeuksia tiettyihin verkon resursseihin.

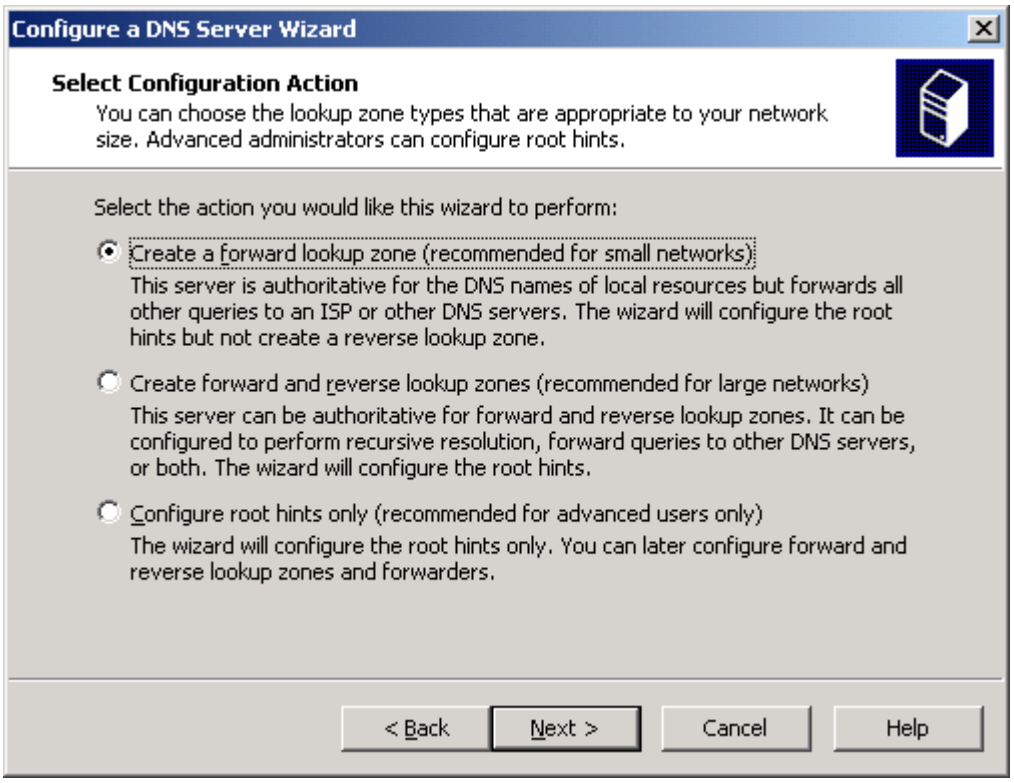
Tämä uusi toimialue tulisi toimimaan jonkin aikaa vanhan toimialueen rinnalla, koska vanha järjestelmä täytyi säilyttää uuden rinnalla niin kauan, että kaikki koneet saatiin liitettyä uuteen toimialueeseen ja kassajärjestelmään. Toinen vaihtoehto olisi ollut liittää uusi Domain Controller osaksi jo olemassa olevaa toimialuetta (kuva 18). Oli kuitenkin selkeintä ja helpointa tehdä aivan uusi toimialue uudelle järjestelmälle.



KUVA 18. Uuden toimialueen luominen

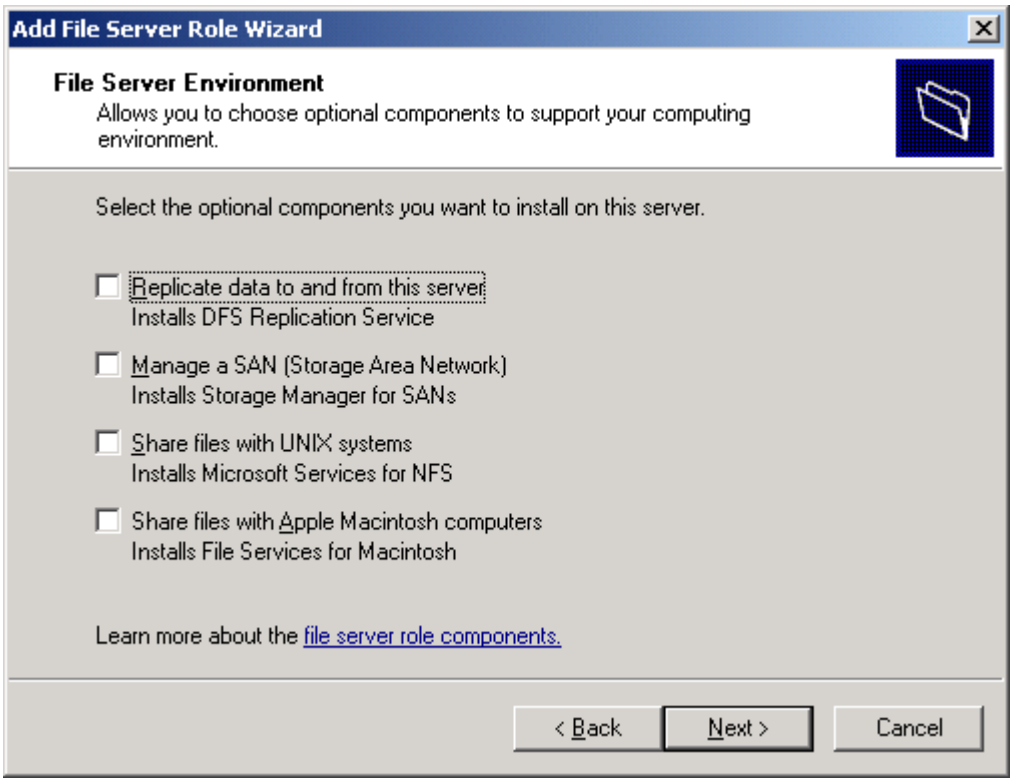
Print Server on rooli, joka hallitsee toimialueeseen liitettyjä verkkotulostimia. Se helpottaa verkonylläpitäjän ja käyttäjän toimia jakamalla esimerkiksi verkkotulostimiksi määritettyjen tulostimien ajureita.

DNS Server rooli toimii verkon nimipalvelimena. Se voidaan määrittää jakamaan muitakin nimitietoja kuin pelkästään toimialueesta löytyviä, mutta koska tässä tapauksessa kyseessä on melko pieni verkko, määritimme sen jakamaan pelkästään toimialueen nimitietoja (kuva 19). Toimialueen ulkopuolisten nimien kyselyt se ohjaa Internet-palveluntarjoajan nimipalvelimelle.



KUVA 19. DNS palvelimen määrittäminen

File Server rooli mahdollistaa tiedostojen jakamisen palvelimelta toimialueen käyttäjille. Sillä pystyy määrittämään tietyille käyttäjille tai ryhmille oikeudet tiettyihin kansioihin tai tiedostoihin. Suurissa verkoissa, joissa on useita palvelimia, File Server voidaan määrittää ylläpitämään jaettuja tiedostoja palvelimilla. Tällöin se jakaa useista eri sijainneista tehtyjä verkkojakokansioita yhdestä loogisesta paikasta, DFS (Distributed File System) kansiosta. File Server mahdollistaa myös tiedostojen jakamisen muiden käyttöjärjestelmien kesken kuin pelkästään Microsoft Windows käyttöjärjestelmä ympäristössä. Koska tämä palvelin tulee suhteellisen pienen verkon käyttöön ja käyttöjärjestelmänä verkon koneissa on Microsoft Windows, niin asensimme File Serverin oletusasetuksilla, jotka mahdollistavat pelkästään tiedostojen jaon Windows-koneiden kesken (kuva 20).



KUVA 20. File Server asennus

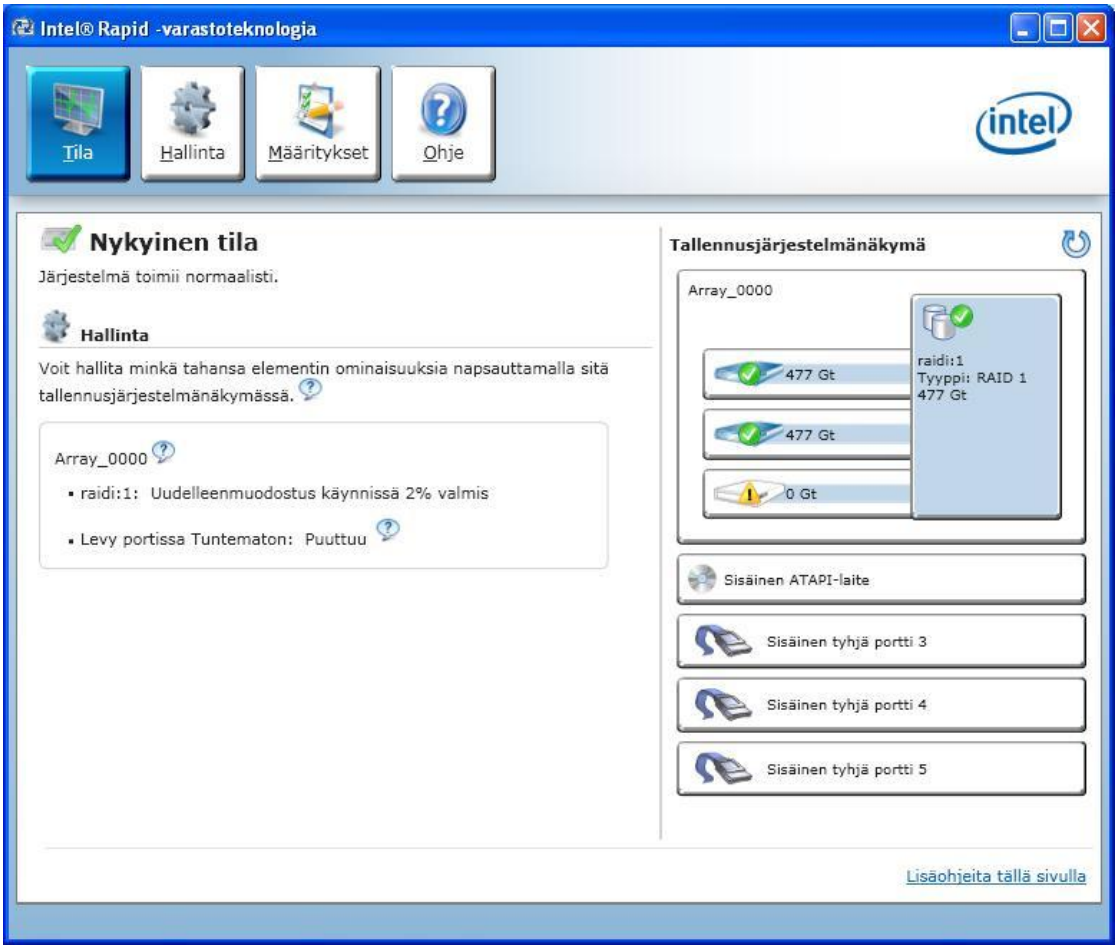
Toimipaikkapalvelimeen asennettiin lisäkiintolevy, johon tehtiin levynpeilaus käyttäen RAID1:stä ja käyttöjärjestelmäksi asennettiin Microsoft Windows XP Pro. Näiden toimien jälkeen tietokoneet jäivät odottamaan Microksen ohjelmien asentamista, jonka he hoitivat etätyöpöytäyhteydellä myöhemmin.

4.2 Toimipaikkapalvelimien kloonaus ja käyttöönotto

Microksen asennettua ohjelmistot toimipaikkapalvelimelle ja pääpalvelimelle oli vuorossa toimipaikkapalvelimen kiintolevyn kloonaaminen kuuteen muuhun tulevaan toimipaikkapalvelimeen. Näihin kuuteen koneeseen oli aikaisemmin asennettu toinen kiintolevy peilausta varten. Koska kloonattavassa koneessa oli käytössä RAID1, päätettiin käyttää tätä hyödyksi.

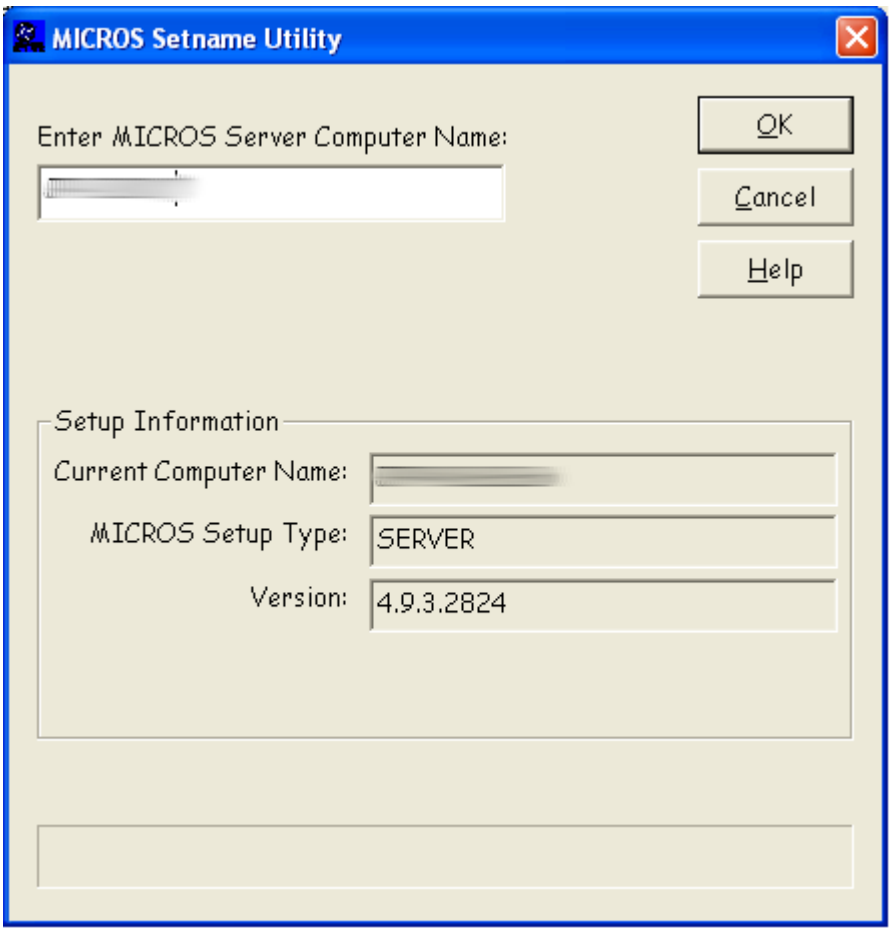
RAID on tekniikka, jolla on mahdollista lisätä tietokoneen kiintolevyjen vikasietoisuutta, tiedonsiirtonopeutta tai näitä molempia. RAID1 on käytännössä tekniikka, jolla lisätään levyjen vikasietoisuutta. Se peilaa jatkuvasti yhden kiintolevyn sisällön toiselle kiintolevylle. Tällöin jos jompikumpi levy hajoaa, tietokone voi yhä käyttää toista ehjää levyä. RAID1 luo viallisen levyn tilalle vaihdettuun uuteen levyyn uuden levynpeilauksen ja tätä ominaisuutta käytettiin hyväksi kloonauksia tehtäessä. Eli käytän-

nössä peilatun levyn tilalle vaihdettiin vain tyhjä kiintolevy ja järjestelmä teki siihen uuden peilauksen (kuva 21). Tällöin levylle siirtyi niin käyttöjärjestelmä kuin Microksen asentama kassajärjestelmä tietokantoineen. Tämä toistettiin jokaisen koneen päälevynkohdalla kohdalla ja päälevyjen takaisin laiton jälkeen, tekivät ne peilaukset koneisiin asennettuihin varalevyihin ja näin saatiin seitsemän kloonattua toimipaikkapalvelinta. Ainut huono puoli tässä käytetyssä järjestelyssä oli peilauksen hitaus. Yhden koneen kiintolevyjen peilaaminen kesti 5-6 tuntia.



KUVA 21. Kiintolevyn peilaus

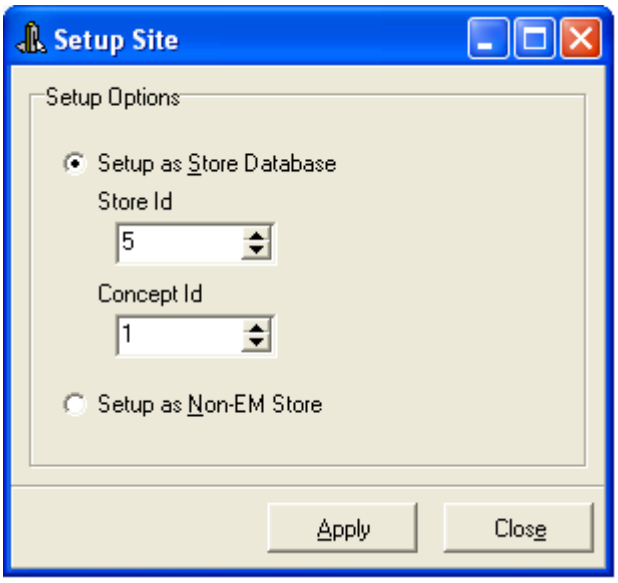
Koska toimipaikkapalvelimet olivat tässä vaiheessa toistensa kopioita, tarvitsi niihin asennetun kassajärjestelmän asetuksia muuttaa, jotta ne saataisiin yksilöityä toimipaikkakohtaisiksi. Muutokset toteutettiin Microkselta saadun ohjeen mukaisesti ja muutokset aloitettiin toimipaikkapalvelimen nimen vaihtamisesta. Nimi täytyi vaihtaa Microksen ohjelmasta käsin (kuva 22), jotta nimen muutos vaikutti koko kassajärjestelmään eikä pelkästään käyttöjärjestelmään.



KUVA 22. Toimipaikkapalvelimen nimen muuttaminen

Tämän jälkeen purettiin Microkselta saatu zip-paketti palvelimelle. Zip-paketti sisälsi skriptit muun muassa alennuskorttien käyttöön järjestelmässä sekä ohjelman paikallisten raporttien tekoon. Mitään ei tarvinnut varsinaisesti asentaa zip-paketista vaan riitti kun sen purki C-aseman juureen. Zip-paketti sisälsi myös paljon muitakin Microksen ohjelmia/skritptejä, joista minulla ei ole tämän tarkempaa tietoa.

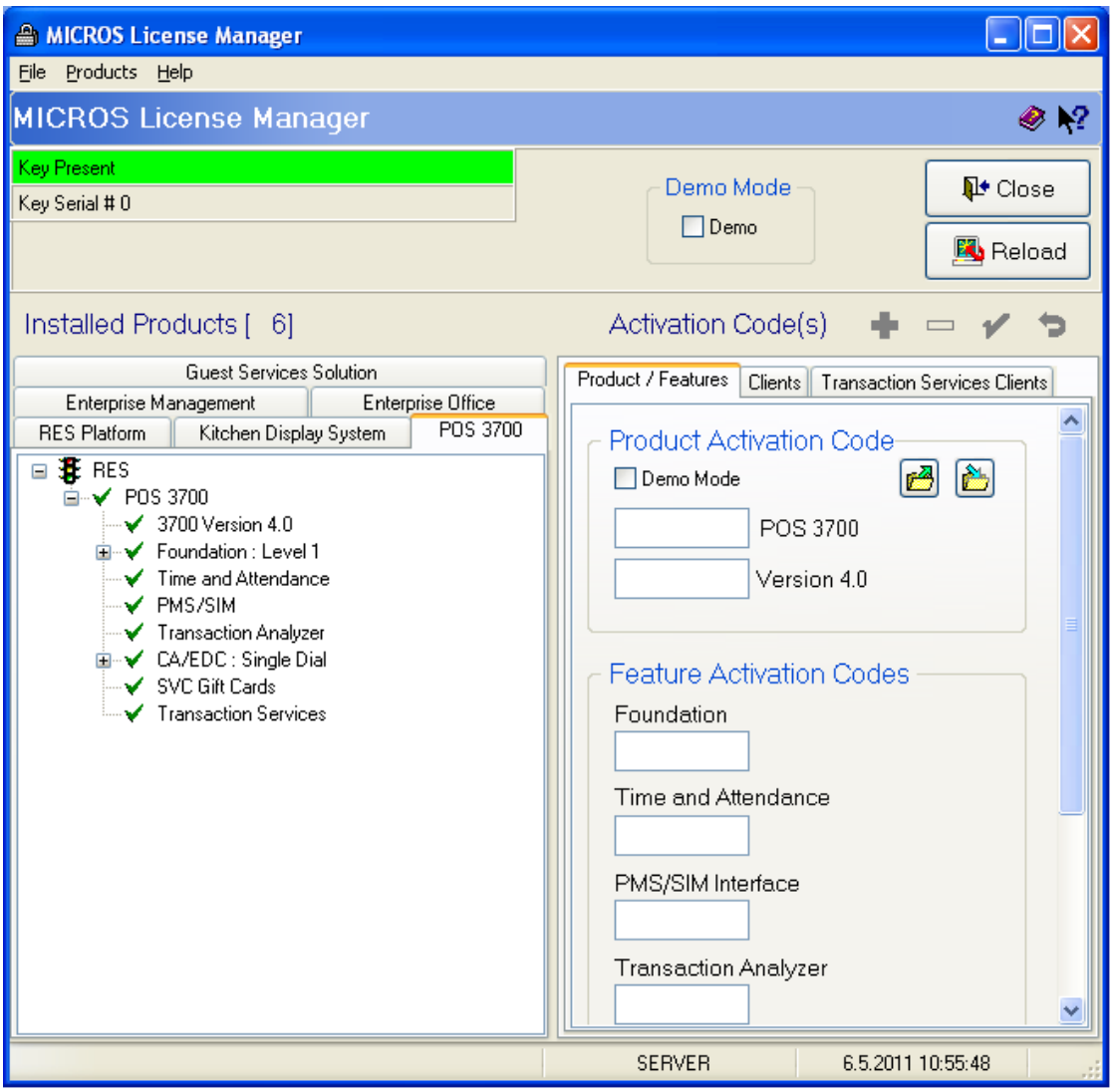
Seuraavaksi määritettiin toimipaikkapalvelimelle sekä toimipaikalle tunniste (kuva 23), jonka mukaan pääpalvelin osaa tunnistaa toimipaikan ja yhdistää sen oikeaan tietokantaan. Nämä tunnisteet olivat Microksen aikaisemmin pääpalvelimen tietokantaan määrittelemiä ja ne ovat järjestelmän toiminnan kannalta oleellista.



KUVA 23. Toimipaikkatunnuksen asettaminen

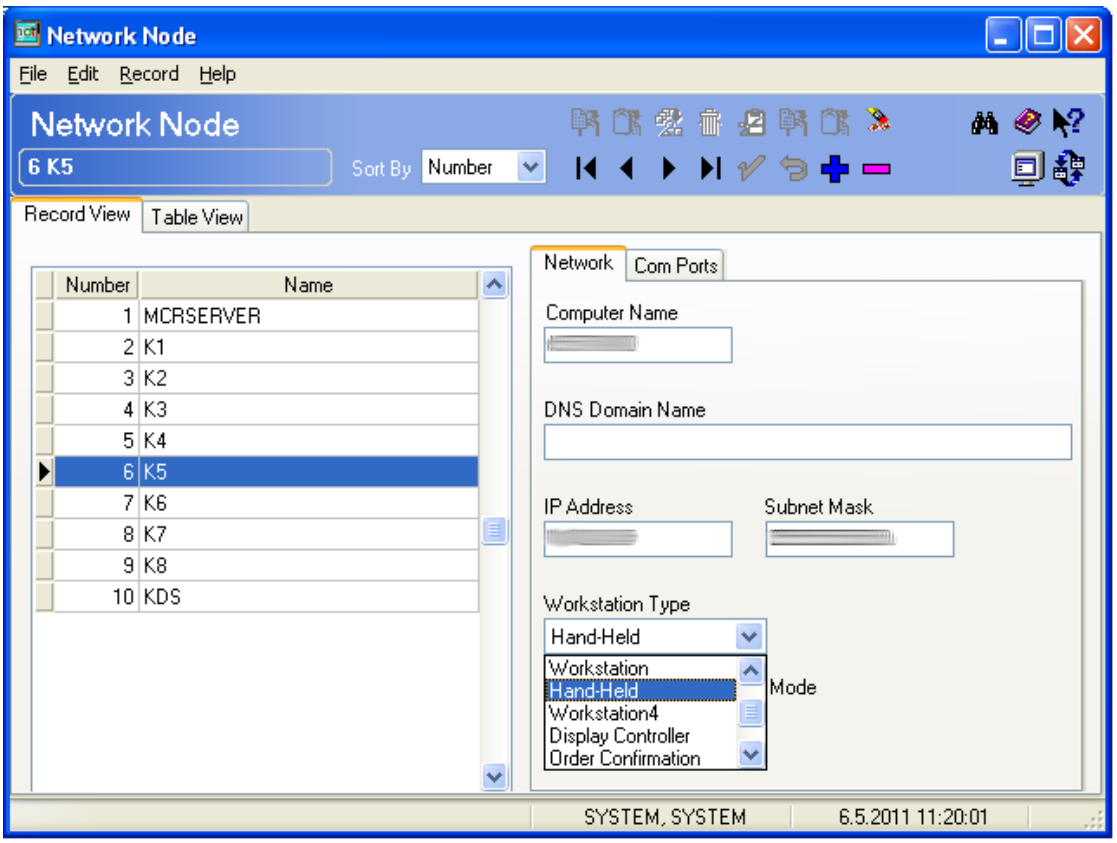
Toimipaikkatunnisteen määrittämisen jälkeen, toimipaikkapalvelimelle syötettiin lisenssit, joilla aktivoitiin itse järjestelmä sekä tarvittavat palvelut toimipaikan kassajärjestelmästä (kuva 24). Nämä lisenssit järjestelmä tarkisti koneeseen liitetystä USB-lisenssiavaimesta, joka on kullekin toimipaikalle yksilöllinen. Kaikille toimipaikoille oli myös oma lisenssilistansa, joka mahdollisti eri palveluiden käyttämisen eri toimipaikoissa.

Järjestelmä tarvitsee toimiakseen edellä mainitun USB-avaimen, joten sen täytyy olla koneessa kiinni jatkuvasti. Jos se syystä tai toisesta hajoaisi, toimii järjestelmä seitsemän päivän ajan ilman sitä. Seitsemän päivän jälkeen järjestelmä lukittuu jos korvaavaa USB-avainta ei ole liitetty tietokoneeseen.



KUVA 24. Lisenssien syöttö

Viimeisenä toimena oli toimipaikan kassalaitteiden lisääminen toimipaikkapalvelimen tietokantaa (kuva 25). Näitä laitteita olivat esimerkiksi kassapäätteet, kuittitulostimet ja käsikassat. Kullekin kassalaitteelle tuli määrittää yksilöllinen nimi, kiinteä IP-osoite sekä oliko kyseessä kassapääte, kuittitulostin jne. Lisätessä laitteita tietokantaan täytyi kirjata ylös laitteiden nimet sekä niihin liitetyt IP-osoitteet, koska toimipaikan käyttöönotossa täytyy tiettyihin laitteisiin määrittää vastaavat nimet ja IP-osoitteet.



KUVA 25. Kassalaitteiden lisäys järjestelmän tietokantaan

Näillä toimilla saatiin toimipaikkapalvelin valmiiksi käyttöönottoa varten. Kuitenkin ennen kuin ensimmäinen toimipaikka voitiin ottaa käyttöön uudella järjestelmällä, täytyi pääpalvelin saada ensin toimintaan ja liitettyä yrityksen verkkoon.

4.3 Pääpalvelimen liittäminen verkkoon

Varsinaiset verkonmuutostyöt aloitettiin toimistolla sijaitsevan uuden kassajärjestelmän pääpalvelimen liittämisellä verkkoon. Koska toimipaikkoja oli useita ja kassajärjestelmän toimiminen on näiden toimipaikkojen liiketoiminnan kannalta ehdottoman tärkeää, päätettiin jättää vanhat palvelimet vielä tässä vaiheessa uuden rinnalle. Näin myös vanha kassajärjestelmä toimisi sen aikaa kunnes tarvittavat muutokset kassojen, maksupäätteiden ja työasemien liittämiseksi uuteen järjestelmään viimeisessäkin toimipaikassa olisivat tehty.

Koska palvelimeen oli tässä vaiheessa jo asennettu tarvittavat palvelut, Microksen kassajärjestelmä ohjelmineen ja tarvittavat tietokannat oli siirretty siihen, jäi oikeastaan jäljelle vain palvelimen liittäminen verkkoon. Tämä tarkoitti käytännössä kiintei-

den IP-osoitteiden määrittämistä palvelimelle sekä palvelimen liittämistä yrityksen sisäverkon kytkimeen. Tämän jälkeen oli mahdollista liittää ensimmäinen toimipaikka uuteen järjestelmään.

4.4 Ensimmäisen toimipaikan liittäminen uuteen järjestelmään

Alkuperäinen suunnitelma oli aloittaa ensimmäisen toimipaikan liittäminen järjestelmään maanantaipäivänä, koska kyseinen toimipaikka on auki torstaista lauantaihin. Tällöin olisi jäänyt kolme päivää aikaa testata järjestelmän toimintaa sekä puuttua mahdollisiin epäkohtiin. Johtuen kuitenkin Microksen aikatauluista aloituspäivä siirtyi torstaille, joten laitteet ja järjestelmät täytyi saada toimimaan yhden päivän aikana ja järjestelmän testaus suoritettaisiin käytön yhteydessä.

Koska kaikki toimipaikat olivat samassa IP-osoiteavaruudessa, käytettävissä oleva IP-osoitteet oli jaettu toimipaikkojen kesken siten, että kunkin toimipaikan IP-osoitteet alkaisivat tasakymmenistä. Näin saataisiin looginen osoiteavaruus, jolloin päällekkäisiä IP-osoitteita olisi helpompi välttää.

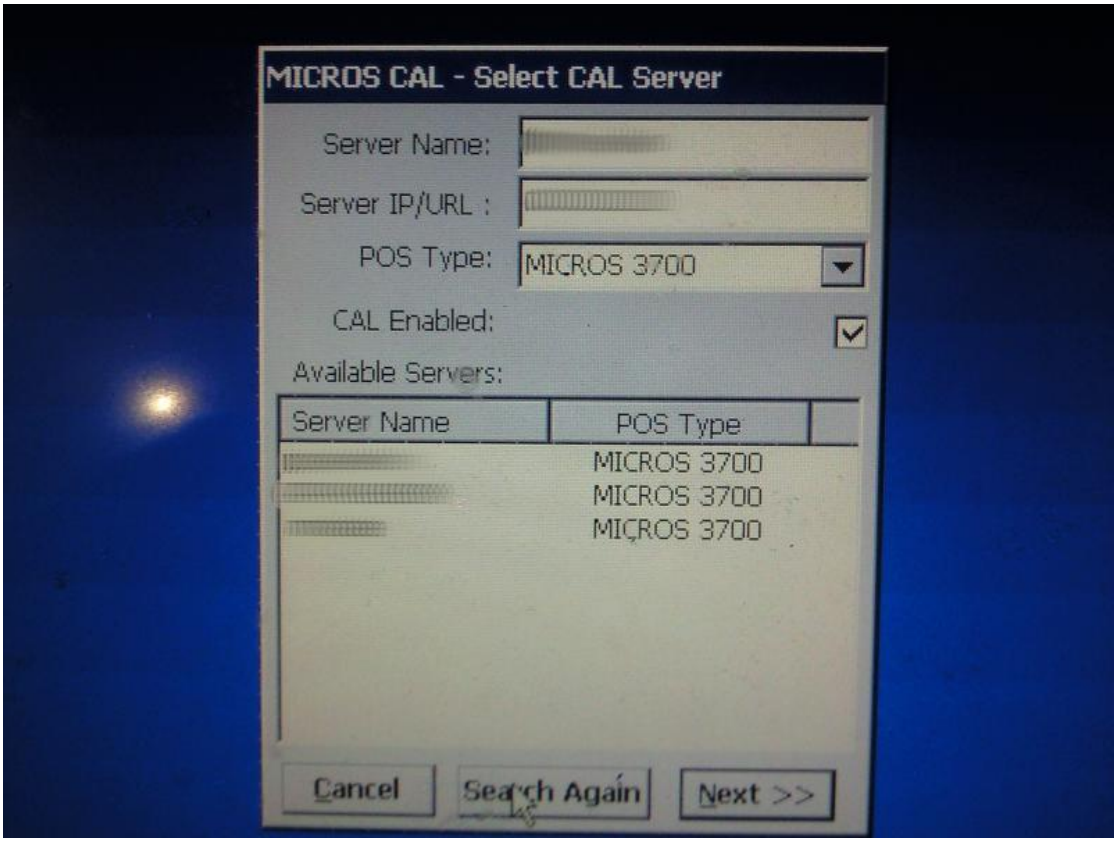
Ensimmäinen toimipaikassa tehtävä asia oli Consept10 lähiverkkoratkaisun poistaminen käytöstä. Tämä tarkoitti käytännössä yhden kytkimen siirtämistä SHDLS-verkon kytkimeen kiinni. Tämä toimenpiteen jälkeen kyseisen toimipaikan kaikki tietoliikenne kulki SHDSL-verkon kautta toimistolle ja sieltä tarvittaessa Internetiin. Samoin kuin vanha kassajärjestelmä myös Consept10:n lähiverkkoratkaisua ei voitu vielä tässä vaiheessa katkaista kokonaan pois käytöstä vaan se tehtäisiin vasta kun kaikkien toimipaikkojen liikenne kulkisi SHDLS-verkon kautta.

Tämän jälkeen uusi toimipaikkapalvelin liitettiin toimipaikan verkkoon kiinni. Koska siihen oli jo aikaisemmin asennettu tarvittavat ohjelmistot sekä tarvittavat asetukset, riitti ainoastaan kiinteän IP-osoitteen määrittäminen ja verkkokaapelin liittäminen tietokoneeseen. Tämän jälkeen järjestelmä oli valmis siihen liitettäviä kassalaitteita varten.

Kassalaitteiden liittäminen järjestelmään aloitettiin kassapäätteistä, joita oli neljä kappaletta kyseisessä toimipaikassa. Kassapääte on periaatteessa kosketusnäytöllinen tietokone, jossa on käyttöjärjestelmänä Microsoft Windows CE 6.0. Kassapäätteestä it-

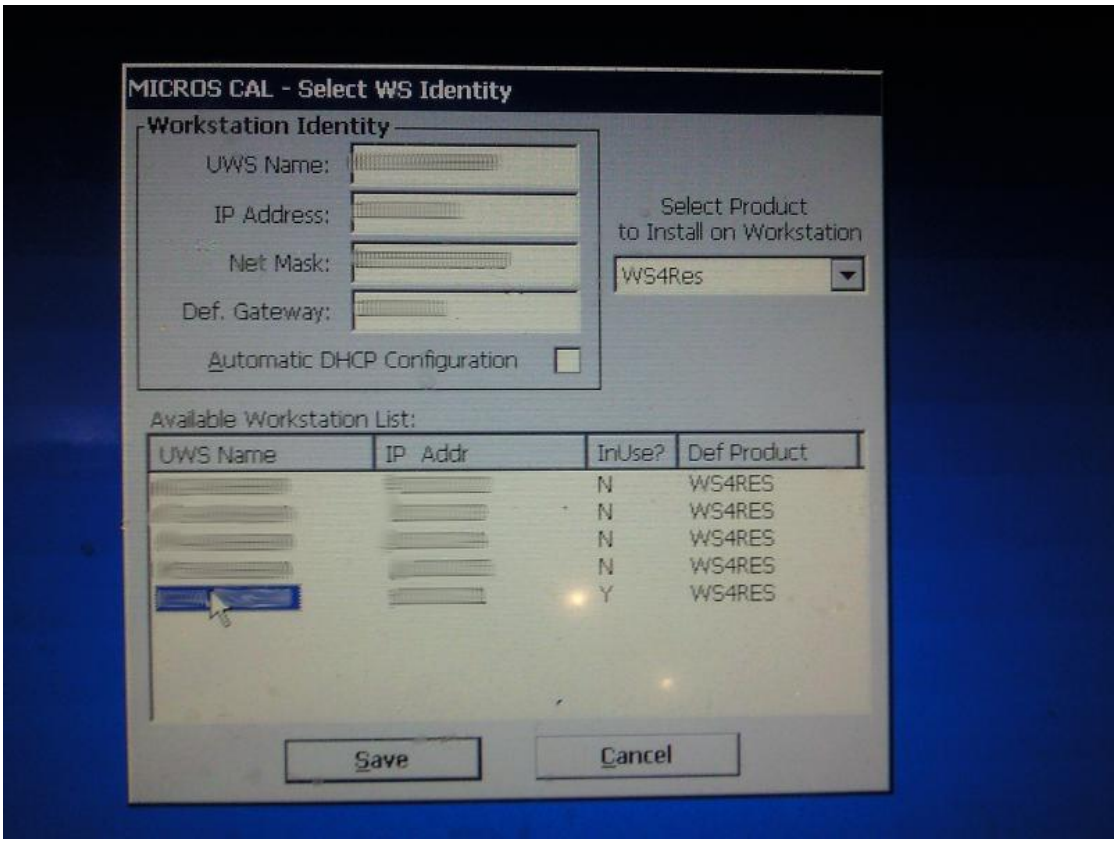
sestään löytyy siihen asennettu kassajärjestelmä sekä tähän kuuluvat oheislaitteet muun muassa kortinlukija. Tarvittaessa tällainen kassapääte voitaisiin korvata tavallisella tietokoneella, johon on asennettu Microsoft Windows XP Pro sekä siinä tulisi olla kosketusnäyttö.

Ensimmäinen toimenpide kassapäätteiden liittämisessä oli vanhan kassaohjelmiston poisto laitteesta. Tähän tarkoitukseen käytettiin Wipe Compact Flash Utility-nimistä ohjelmaa (WCF). Tämän jälkeen kassapääte käynnistettiin uudelleen, jolloin se automaattisesti alkoi etsiä verkosta mahdollista palvelinta, josta se saisi haettua uuden version kassaohjelmistosta. Aluksi ilmeni ongelmia palvelimen löytymisessä, sillä tässä vaiheessa pitäisi laitteen listauksessa näkyä niin toimistolla sijaitseva pääpalvelin kuin toimipaikkapalvelin. Laite ei aluksi löytänyt näistä kuin toimiston pääpalvelimen. Vika oli ilmeisesti aikaisemmin siirretyn kytkimen johdotuksessa, sillä vika korjaantui kytkimen kaikkien verkkokaapeleiden uudelleen kytkennän jälkeen. Korjauksen jälkeen laitteen listalta löytyi niin toimiston palvelin kuin toimipaikkapalvelin (kuva 26).



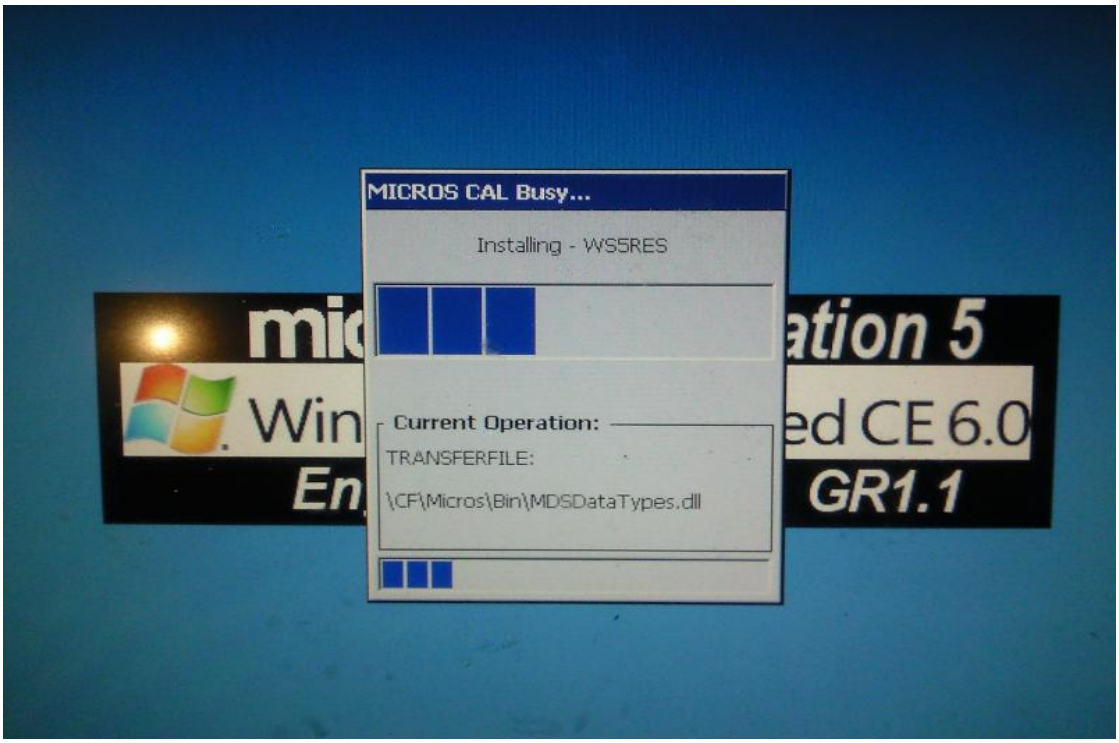
KUVA 26. Kassapäätteelle näkyvät kassapalvelimet

Palvelimen valinnan jälkeen näytölle ilmestyi lista toimipaikkapalvelimen tietokantaan tehdyistä laitteista. Listasta valittiin se laite jona kyseinen kassapääte haluttiin toimipaikkapalvelimeen liittää, tässä tapauksessa kassa 1 (kuva 27).



KUVA 27. Kassapäätteen liittäminen toimipaikkapalvelimeen

Seuraavaksi kassapääte latasi palvelimelta uuden kassaohjelmiston ja asensi sen (kuva 28), jonka jälkeen kassapääte oli valmis palvelemaan asiakkaita (kuva 29). Kahden kassapäätteen asennuksessa ilmeni ongelmia. Kesken kassaohjelman asennuksen verkkoyhteys palvelimeen katkesi, jolloin myös ohjelman lataus keskeytyi. Vika löytyi pienen ihmettelyn jälkeen. SHDSL-verkkoon liitetyn kytkimen virtajohto oli päässyt irtoamaan ja kaikki kyseisen kytkimen kautta kulkevat yhteydet olivat poikki. Kytkimen päälle laiton jälkeen, kassaohjelmiston määrittely ja asennus jouduttiin suorittamaan uudestaan näissä kahdessa kassapäätteessä.



KUVA 28. Kassaohjelmiston asennus kassapäätteelle

KUVA 29. Toimintavalmis kassapääte

Kassapäätteiden liittämisen jälkeen oli vuorossa maksupäätteiden asetusten muuttaminen (kuva 30). Tässä toimipaikassa maksupäätteet käyttivät aikaisemmin Concept10:n

lähiverkkoa liikennöidessään pankin palvelimien kanssa, eli niihin täytyi muuttaa IP-osoitteet vastaamaan uutta verkkoratkaisua. Maksupäätteissä on mahdollista käyttää DHCP:tä IP-osoitteiden hakemiseen, mutta päätettiin kuitenkin laittaa kiinteät IP-osoitteet näihinkin laitteisiin. Tämä siksi, että saataisiin loogisesti jaoteltua IP-osoitteet kullekin toimipaikalle.

KUVA 30. Maksupäätteen asetusten muuttaminen

Tämän jälkeen asennettiin käsikassoihin kassajärjestelmä sekä tehtiin tarvittavat muutokset käsikassoihin liittyviin kuittitulostimiin. Käsikassoihin järjestelmän asennus toimi saman kaavan mukaan kuin kassapäätteisiin ainoana erona oli, että ne täytyi liittää tiettyyn kuittitulostimeen. Kuittitulostimiin riitti IP-osoitteiden uudelleen määritys.

Ensimmäisen toimipaikan testausajan jälkeen on tarkoitus toteuttaa vastaava muutos yrityksen muihinkin toimipaikkoihin. Muutos tullaan toteuttamaan samanlaisesti kuin ensimmäisessä toimipaikassa kuitenkin ilman ensimmäisen toimipaikan vaatimaa kahden viikon mittaista järjestelmän testausta. Tämän lisäksi on vielä tehtävä muutokset toimipaikkojen työasemien liittämiseksi uuteen toimialueeseen sekä verkkotulostimien ja verkkolevyjen asennus. Itse en ole enää mukana näiden muutosten toteuttamisessa.

5 PÄÄTÄNTÖ

Tämän työn tarkoituksena oli JP-ravintoloille tulevan uuden kassajärjestelmän käyttöönotto sekä samalla yrityksen tietoverkkojen uudistaminen. Verkkojen uudistamisella haettiin olemassa olevien verkkojen yksinkertaistamista sekä turhien päällekkäisyyksien poistamista ja tätä kautta kustannussäästöjä. Asiakkaan suurin tavoite uuden kassajärjestelmän suhteen oli luoda helpommin hallittavissa oleva kokonaisuus toimipaikkojen tuotteiden hinnoitteluun, myynnin raportoimiseen sekä toimipaikkakohtaisten tarjoustuotteiden hinnoitteluun.

Työn tavoitteet kassajärjestelmän käyttöönotossa sekä verkkomuutosten tekemisessä saavutettiin mielestäni hyvin. Uusi kassajärjestelmä vastasi asiakkaan toiveita helpommin hallinnoitavasta kassajärjestelmästä, joka saavutettiin uuden ohjelmiston asentamisella. Verkkomuutoksella tullaan saavuttamaan rahallista hyötyä, kun viimeisen toimipaikan liitämisen myötä Concept10:n lähiverkkoratkaisusta luovutaan.

Tarvittavat verkkomuutokset sekä kassajärjestelmän muutokset saatiin toimintakuntoon ensimmäisessä toimipaikassa, jonka jälkeen opinnäytetyöni ja toimeksiannon aikataulut eivät enää kohdanneet. Alkuperäisten suunnitelmien mukaan, olisin ollut mukana koko prosessissa, mutta työn edetessä ja aikataulujen tarkentuessa, kävi selväksi, että pysyäkseni opinnäytetyöni aikataulussa, en voisi olla mukana toimeksiannon loppuun saattamisessa. Ensimmäisen toimipaikan käyttöönotossa käytiin läpi kaikki ne asiat, jotka tullaan toistamaan muissa toimipaikoissa, joten opinnäytetyöni sisältää toimeksiannon oleelliset osat ja ei siksi jää vajaaksi.

Suurin haaste tässä työssä oli mielestäni työn laajuus ja se, että hankkeessa oli useita eri toimijoita ja vaiheita. Yhdellä toimijalla saattoi olla useita perättäisiä työvaiheita, joista toisten toimijoiden työn eteneminen oli riippuvaista. Tällöin aikataulujen sovitus oli välillä hieman hankalaa. Tällaisia vaiheita oli esimerkiksi uuden järjestelmän tietokantojen toteutus, sillä tiedot jouduttiin siirtämään vanhoista tietokannoista osittain niin sanotusti käsipelillä ja tämä oli aikaa vievää työtä.

Asiakas on ollut tyytyväinen järjestelmän toimintaan niin kassajärjestelmän kuin myös verkkoratkaisujen osalta. Nähtäväksi tosin jää, kuinka hyvin SHDSL-verkko tulee toimimaan kaikissa toimipaikoissa vai tarvitaanko kyseisiin toimipaikkoihin vielä

ADSL-liittymät lisäksi. Toimipaikkojen kaikki liikenne tulee kulkemaan SHDSL-verkon kautta, jolloin verkko voi ruuhkautua. Myös etäisyydet toimipisteen ja toimiston välillä voi kasvaa liian suuriksi, mikä heikentää huomattavasti verkon suorituskykyä. Tällöin ADSL-liittymä voisi taata varmemman yhteyden esimerkiksi maksupäätteitä varten.

Toimeksianto oli mielestäni hyvin opettavainen kokemus. Siinä pääsi näkemään monivaiheisen projektin etenemistä ja osallistumaan sen toteutukseen. Työssä tuli tutuksi niin palvelimet, toimipaikkojen kassalaitteet kuin myös kyseinen kassajärjestelmäkin sekä erilaiset verkkoratkaisut. Toimeksianto antoi kuvan projekteista, joita tulevaisuudessa tulen mahdollisesti työni kautta toteuttamaan ja siksi se luo hyvän pohjan osaamiselleni.

LÄHTEET

1. Saarelainen, Kari. Lähiverkkojen tekniikka. Espoo: Suomen ATK-kustannus Oy. 1993.

2. Suoranta, Lauri. WWW-dokumentti. http://www.tietokone.fi/lehti/tietokone_10_2008/kuitua_ja_kuparia_684. Päivitetty 10/1008. Luettu 13.4.2011.

3. Kuva UTP- ja STP-kaapeleista. WWW-dokumentti. http://dharmawanalfian.files.wordpress.com/2010/08/utp20and20stp.jpg. Ei päivitystietoja. Luettu 24.4.2011.

4. Wireless Distribution System. WWW-dokumentti. http://en.wikipedia.org/wiki/Wireless_Distribution_System. Päivitetty 31.3.2011. Luettu 25.4.2011.

5. Kuva WDS:n toiminnasta. http://en-us-support.belkin.com/euf/assets/images/answer/router/wds.gif. Ei päivitystietoja. Luettu 13.5.2011.

6. Tuominen, Jukka. Optinen tiedonsiirto. Essee. Teknillinen korkeakoulu. WWW-dokumentti. http://www.tml.tkk.fi/Studies/Tik-110.300/1998/Essays/ots. 5.4.1999. Ei päivitystietoja. Luettu 13.4.2011.

7. Fiber Optics. WWW.dokumentti. http://www.arcelect.com/fibercable.htm. Ei päivitystietoja. Luettu 15.3.2011.

8. Hakala, Mika, Vainio, Mika. Tietoverkon rakentaminen. Jyväskylä: Docento Finland Oy. 2005.

9. Bridging And Switcing Basics. WWW-dokumentti. http://docwiki.cisco.com/wiki/Bridging_and_Switching_Basics. Päivitetty 17.12.2009. Luettu 8.4.2011.

10. Aliverkko. WWW-dokumentti. http://fi.wikipedia.org/wiki/Aliverkko. Päivitetty 3.5.2010. Luettu 11.4.2011.

11. Perimutter, Bruce & Zarkower, Jonathan. Virtuaaliset yksityisverkot. Suom Timo Kokkonen. Helsinki: Edita Oyj. 2000.

12. VPN. WWW-dokumentti. http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/vpn.html. Päivitetty 27.9.2007. Luettu 9.4.2011.

13. Moore, Brandon. VPN Authentication. Word-dokumentti. brandonr-moore.com/docs/VPNAuthentication.doc. 2008. Ei päivitystietoja. Luettu 15.3.2011.

14. Cisco Systems, Inc. Fundamentals of Network Security. Indianapolis: Cisco Press. 2004.

15. QoS Pre-Classify and End-to-End QoS. WWW-dokumentti. http://www.chainringcircus.org/qos-pre-classify-and-end-to-end-qos/. Päivitetty 23.11.2009. Luettu 17.3.2011.

16. Layer 2 Tunnel Protocol. WWW-dokumentti. http://www.cisco.com/en/US/docs/ios/12_0t/12_0t1/feature/guide/l2tpT.html. Ei päivitystietoja. Luettu 17.3.2011.

17. Layer 2 Tunneling Protocol. WWW-dokumentti. http://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol. Päivitetty 6.5.2011. Luettu 17.3.2011.

18. L2TP Support. WWW-dokumentti. http://www.zyxel-tech.de/snotev120/refer/l2tp_spt.htm. Ei päivitystietoja. Luettu 17.3.2011.

19. TCP-Protocol. WWW-dokumentti. http://en.kioskea.net/contents/internet/tcp.php3. Päivitetty 16.8.2008. Luettu 19.3.2011.

20. Different VPN Tunnel Types In Windows. WWW-dokumentti. http://blogs.technet.com/b/rrasblog/archive/2009/01/30/different-vpn-tunnel-types-in-windows-which-one-to-use.aspx. Ei päivitystietoja. Luettu 18.3.2011

21. L2TP/IPsec Tunnels. WWW-dokumentti. http://www.juniper.net/techpubs/software/erx/junose53/swconfig-routing-vol1/html/l2tp-over-ipsec-config4.html. Ei päivitystietoja. Luettu 20.3.2011.

22. PPTP. WWW-dokumentti. http://fi.wikipedia.org/wiki/PPTP. Päivitetty 8.2.2011 luettu 24.4.2011.

23. SSL-VPN. WWW-dokumentti. http://searchsecurity.techtarget.com/definition/SSL-VPN. Päivitetty 20.6.2006. Luettu 19.3.2011.

24. Transport Layer. WWW-dokumentti. http://en.wikipedia.org/wiki/Transport_Layer_Security. Päivitetty 12.4.2011. Luettu 20.4.2011.

25. Virtual Private Network. WWW-dokumentti. http://www.jungo.com/openrg/doc/5.3/user_guide/html/html_openrg_user_manual/sect_vpn.html. Ei päivitystietoja. Luettu 19.3.2011.

26. Understanding SSL VPN. http://palisade.plynt.com/issues/2006Jul/ssl-vpn/. Ei päivitystietoja. Luettu 20.4.2011.

27. Virtual Private Networking. WWW-dokumentti. http://www.pugetsound.edu/about/offices--services/technology-services/help--support/self-help/vpn/. Ei päivitystietoja. Luettu 20.3.2011.

28. Mikä on AD Domain Cotroller. WWW-dokumentti. http://itpro.fi/wiki/sivut/Identiteetti%20ja%20hakemistot/Mik%C3%A4%20on%20AD%20Domain%20Controller.aspx. Ei päivitystietoja. Luettu 28.4.2011.